INSTITUTE FOR LABOUR LAW
BLIJDE-INKOMSTSTRAAT 17 BUS 3423
3000 LEUVEN, BELGIUM
FRANK.HENDRICKX@KULEUVEN.BE

Report

29 July 2021

From: Frank Hendrickx, Simon Taes – KU Leuven
To: Sarah Kamer – European Cockpit Association

Study "GDPR-project" of KU Leuven for the European Cockpit Association (*ref. VS/2019/0291)*

Report Title:

Data protection law and the exercise of collective labour rights by trade unions vis-à-vis employers or groups of employers in a transnational context

Authors: Frank Hendrickx & Simon Taes, Institute for Labour Law – KU Leuven

This document contains the analysis resulting from the project study conducted by KU Leuven for the European Cockpit Association under the agreement with reference *VS/2019/0291.*

Following the project assignment, this draft aims to identify concrete situations when GDPR and data protection interfere with the collective bargaining process; assess whether appropriate tools, rules are in place at national and European level to facilitate/overcome those situations; identify relevant best practices from other industries, especially those examples with a transnational dimension.

European Commission

This publication has been produced with the financial support of the European Commission, under the call for proposals VP/2019/002, "Information and training measures for workers' organisations". The project is called "Transnational Agreements - Best practice and feasibility." The contents of this publication are the responsibility of the European Cockpit Association and the guest authors and are in no way be taken to reflect the views of the European Commission.

Table of contents

Introduction 4
Scope and objectives 4
Industrial relations experiences 4
Structure and methodology 5
Chapter 1. Legal frameworks 7
1.1. Data protection frameworks: the GDPR and beyond 7
1.2. A strong fundamental rights foundation – coherent systems 9
1.3. Specific guidance for data protection in the work environment 10
1.4. Key findings 11
Chapter 2. Data protection standards and information rights 12
2.1. Foundations data protection standards 12
2.2. The market function of personal data standards 13
2.3. Freedom of information as a fundamental right 15
2.4. Conflict of fundamental rights 16
2.5. Information rights in industrial relations 18
a. Sources on information and consultation 18
b. Sources on collective bargaining 21
c. Confidentiality 22
2.6. Benchmark cases 24
a. Works council 24
b. Equal pay 26
2.7. Key findings 27
Chapter 3. HR and IR justifications under the GDPR framework 28
3.1. Introduction 28
3.2. Legitimacy 28
a. General 28
b. Legal obligation 30
c. Performance of a contract 32
d. Legitimate interest 32
e. Consent 34
d. Sensitive data 35
3.3. Proportionality 36
3.4. Purpose limitation 38
a. Principle 38
b. Compatibility assessment for secondary use 38
c. Compatibility levels 39
d. Additional safeguards 41
e. Purpose specification 42
3.5. Access to personal data 43
a. Access 43
b. Rectification 44
c. Evaluation data 44
d. Erasure 45
e. Data portability 45
3.6. Key findings 46
Chapter 4. Governance and tools for GDPR compliance 48
4.1. Introduction 48
4.2. Installing a GDPR compliance culture 48
Privacy by design and by default 48
Shadowing DPIA 49

4.3. Toolbox-questions 51
Q1: Which (personal) data flows can be identified ? 52
a. Analysis 52
b. IR models 52
c. Model scenarios 52
d. Model-levels 53
e. Data flow chart 54
c. Key findings 55
Q2: Who is identified as controller/processor/recipient ? 55
a. Analysis 55
b. Application 58
c. Key findings 62
Q3: What is the legal/legitimate ground of personal data processing? 63
a. Analysis 63
b. Application 67
c. Key findings 72
Q4: Which (personal) data are communicated to the workers' representatives and for which purposes? 72
a. Analysis 72
b. Application 74
c. Key findings 76
Q5: How is personal data processing minimized to what is necessary and proportionate? 76
a. Analysis 76
b. Application 77
c. Key findings 79
Q6: Have data subjects been informed ? 79
a. Analysis 79
b. Application 81
c. Key findings 82
Q7: What is the territorial scope of the personal data processing? 83
a. Analysis 83
b. Application 86
c. Key findings 86
Q8: Are risks to the rights and freedoms of data subjects properly addressed ? 87
a. Analysis 87
b. Application 88
c. Key findings 88
Q9: Are additional guarantees applicable ? 89
a. Analysis 89
b. Application 91
c. Key findings 91
Q10: Have interested parties been involved ? 92
a. Analysis 92
b. Application 93
c. Key findings 94
Conclusions, recommendations and toolbox 96
General 96
Chapter findings 96
Recommendations and solutions 98
Annex 100

Introduction

Scope and objectives

The main purpose of this study is to find out whether and how the European Cockpit Association (ECA) and workers' representatives can challenge employers who decline to provide information on the grounds of data protection legislation or on the grounds of commercial confidentiality.

The study is conducted for the European Cockpit Association (ECA), the representative organisation of European pilots at European Union (EU) level, representing pilots from the national pilot associations in a large number of European countries.

This study will take into account this context and do so in light of the need to respect fundamental rights (including information rights) and the need to provide guidance and reassurance to both sides of the industry in order to secure the effective and lawful functioning of industrial relations where information can be exchanged in a legitimate manner. It is assumed that the conduct of effective industrial relations relies on the ability of representatives to obtain the information required for successful negotiations, consultations and collective bargaining.

This study concentrates on data protection laws and principles, mainly departing from the perspective of the 'General Data Protection Regulation', known as the GDPR, and brings it in connection with collective labour rights and industrial relations, mainly from the view of the right to information and consultation as well as the right to collective bargaining.

Within the main project study and scope, the main research question can be summarized as: to what extent can data protection laws and regulations (in particular the GDPR) pose limits to the exercise of the right to information in a collective labour rights context where trade unions face employers or groups of employers in a transnational context.

From this question, a number of legal issues, problems and questions can be identified.

Industrial relations experiences

In the context of industrial relations, a number of information or personal data are desired for different purposes. On the basis of assumed cases as well as reported experiences from different members, the following examples can be given.

- A main purpose relates to the exercise of the right to information in order to **conducting consultations and negotiations** with employers. Information related to financial/ company data, required to conduct the collective bargaining process, is not always set out in annual reports, accounts or other publicly available documents. Such information relates, for example, to payroll data, pension contributions, total number of workforce and breakdown (rank, length of service, full/part-time, etc.), total numbers and averages of age per category, duty hours per year. The question is how representatives may obtain this information from the company.
- One purpose relates to the follow up on the **implementation of working conditions** following from legislation or as collectively agreed. For example, information is required for ensuring that a collective agreement regarding seniority has been correctly implemented; that a collective agreement on scheduling / rostering has been correctly applied; to monitor for transparency and fairness purposes; or to monitor Flight Data Monitoring (FDM) agreements. Access to information may also be needed to comply with duties under Health and Safety legislation. For example, a reported experience relates to a refusal, based on the GDPR to give access to rosters to compare distribution of flying hours/times.

- Some purposes may relate to **human resources practices** in which trade unions may have an interest. For example, an issue on holiday planning has been reported, where vacations were either directly assigned or where a vacation list is negotiated and agreed with unions. In both cases, personal data protection may become an issue if unions wish to verify whether holidays are fairly distributed among employees and what criteria are used.
- In the context of **collective dismissal**, information needs arise, not only for employers to comply with legal requirements, but also in order for trade unions or workers' representatives to conduct consultations or negotiations. For example, it has been reported that, where workers' representatives aimed to mitigate the consequences of a collective dismissal procedure, the employer refused to provide a full list and the points assigned/or evaluation for putting people on the dismissal list.
- In the context of **staff relocation or transfer of undertaking**, also various information needs exist. It has been reported that issues arise with listings and identification of pilots in order to verify whether they have been subject to a transfer or relocation, where some may have been employed through a temporary placement agency. Another reported case concerns the question of a union to proactively receive information about actions already undertaken in moving people to other bases and about changes of contracts, including copies of the contracts (drafts), new planning or new positionings of staff.
- Other purposes relate to the disclosure of **staff related information** in the exercise of collective rights. For example, from the UK it was reported that annual bid results (for fleets), may be published in full and sometimes are published with staff numbers. It may be used and engineered (by a union) to produce an actual list with names of workers. Another bid was shared with the union for reasons of transparency but not with the pilots concerned. The reason was obviously confidentiality and gaining trust from the union, but could also have a negative effect on generating mistrust (among pilots) in the union if not handled properly.
- Another issue is the **assistance of trade union members** in individual cases, such as incident, evaluation or disciplinary procedures. For example, an experience was reported where a union representative was denied access to an incident report because of GDPR. The argument was that other employees were mentioned in the report. The employee himself, who originally filed the report, was allowed to see details of the ongoing investigation and the report, but even though he gave his consent, allowing the union (representative) to see this as well, it was denied by the company. This obviously influences the union's possibility to assist/protect its members.
- An increasing relevant purposes is the **use of electronic communication data** and/or the use of the company's resources. For example, it has been reported that unions have had difficulties in sending e-mails to reach all employees, after the company having unfairly accused the union. A related issue is to obtain data about non-members. According to a reported experience in the UK, unions normally poll members only and new entrant data may be a problem, although it can be related to a strike.

Structure and methodology

The wide range of problems, mentioned above, have clear links with the scope and conditions of data protection regulation, in particular the GDPR. Therefore, in this study, we will discuss the potentials and limitations of data or information flows in light of the GDPR, linking this to the employment and industrial relations context and purposes.

While data protection standards are round for some decades, the GDPR is a rather recent instrument. Furthermore, the field of personal data protection in employment and industrial relations is a relatively

specific field. The questions raised in this study are, therefore, not yet fully developed in current legal systems. In this context, a number of key-steps have to be undertaken in this study:

- **Chapter 1**: The first chapter focuses on legal courses and specifics for the HR context. The legal frameworks and sources of data protection have to be set out against the broader background of employment and industrial relation. In discussing the key concerns of this study, it is relevant and important to understand the context, origins and perspectives of data protection standards. It is clear that data protection standards give an essential perspective to information flows and exchange. In light of this, the broader setting and the origins of the relevant instruments will be helpful in hard cases and situations where there is room for interpretation or balances need to be struck.
- **Chapter 2**: The second chapter sets the broader narrative and fundamental rights framework and deals with the fundamental conflict between information rights and the right to data protection. It is important to define the relationship between data protection standards and the freedom of information and to establish a narrative for the relation between the GDPR and industrial relations. The right to information (connected with consultations and negotiations) is a collective labour right, not a stand-alone right in the context of data protection. It must be pointed out that, in principle, the GDPR is also based on the free flow of information principle. This foundation may prove to be important as both data protection and free information are fundamental rights. In that context, it is also relevant to position the concept of confidentiality as a limit to free information, and/or as part of data protection, in terms of scope and limits.
- **Chapter 3**: The third chapter focuses on the GDPR and relates to how the major principles of data protection can support HR and IR personal data processing. In order to respond to the issues and problems set out in the introduction and problem analysis, it is relevant to give legitimacy and justification grounds for information and data exchange in the industrial relations context. It must be pointed out that the GDPR provisions are quite open textured and leave room for interpretations. They thus bear potential for the industrial relations context. In this chapter, we also show some benchmark cases where data protection standards and rights to information on HR personal data need to be reconciled.
- **Chapter 4**: The fourth chapter focuses on making information and data exchange in industrial relations scenarios compliant with the GDPR. It gives a governance framework and contains toolbox questions for guiding data flows in industrial relations. A data flow chart will be set up and toolbox questions will lead to various conditions, set under data protection law, to strengthen compliance and make data flows possible.

The analysis is based on the input from ECA and from desk resource including legal sources, such as the GDPR, official documents, other data protection standards, scholarship literature, literature on comparative legal systems.

Chapter 1. Legal frameworks

This chapter focuses on legal courses and specifics for the HR context. The legal frameworks and sources of data protection have to be set out against the broader background of employment and industrial relation. In discussing the key concerns of this study, it is relevant and important to understand the context, origins and perspectives of data protection standards. It is clear that data protection standards give an essential perspective to information flows and exchange. In light of this, the broader setting and the origins of the relevant instruments will be helpful in hard cases and situations where there is room for interpretation or balances need to be struck.

1.1. Data protection frameworks: the GDPR and beyond

The GDPR is a recent instrument. However, it should be noted that the origins of data protection legislation in the European Union go a longer way back in time. The first EU initiative can be found in the Data Protection Directive 95/46/EC, adopted on 24 October 1995,[1] with which the EU created a major legal instrument on the subject.

Also within this 1995 legislation, the scope of application was wide and concerned any operation or set of operations performed upon personal data ('processing'), including collection, storage, disclosure, and so on. Directive 95/46/EC was designed to facilitate the free flow of personal data as well as to provide for a high level of protection, by harmonising the law within the EU in this area.[2] In 2012, however, the European Commission took the initiative to reform the data protection legislation. Taking into account considerations of new technological developments and to make sure that individuals are fully informed about what happens to their personal data and to enable them to exercise their rights more effectively,[3] legal reform was considered necessary.

This led to the adoption of the **'General Data Protection Regulation'**, known as the **GDPR**, on 27 April 2016.[4] The regulation is applicable as from 25 May 2018 and replaces the 1995 Directive. The new GDPR is, furthermore, complemented with a new directive.[5]

> "The GDPR brings some new approaches and shifts in thinking ."

While the whole legal construct of the GDPR looks as new and rather up to date, a number of pre-existing principles have remaind and have not been drastically modified. There is much continuity in the legislative agenda, although the GDPR brings some new approaches and shifts of thinking that need to be taken into account. For example, the concepts of 'privacy by design' and 'privacy by default' shed new light on how data processing needs to be appreciated. Another new concept is 'data minimization', although

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* 23 November 1995, L281/31.
[2] Cf. Recitals 7 to10 Directive 95/45/EC.
[3] COM/2012/09 final.
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *OJ* L 119, 4.5.2016, 1-88.
[5] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ* L 119, 4.5.2016, p. 89-131.

this can also be seen as a translation of the older legitimacy or proportionality principles, as will be explained below.

The EU has not been the only, nor the first, regulator of data protection. The OECD has been one of the first organisations to respond to the increase of automated data processing and the concern to address the issue of data protection with an international instrument. On 23 September 1980, the OECD adopted a **Recommendation concerning guidelines governing the protection of privacy and transborder flows of personal data**. As the title of this recommendation suggests, it concerns a set of guidelines with basic principles of data protection, not a convention. The recommendation is accompanied by an Explanatory Memorandum. As it is explained in paragraph 22 of this Memorandum, the recommendation affirms the commitment of the member countries to protect privacy and individual liberties and to respect the transborder flows of personal data.[6] The OECD updated the guidelines on 11 July 2013.[7] The OECD Guidelines have been very influential and leading in international consensus building. They have exercised a direct influence on the making of national data protection laws around the world.[8]

The Council of Europe adopted a specific **Convention 108** with regard to personal data protection on 28 January 1981.[9] It was the concern of the Member States of the Council of Europe to bring more unity in the national legal systems and to protect the human rights on a higher level throughout Europe.[10] The Convention defines a number of principles for the fair and lawful collection and use of data.

At the time when the EU's data protection, with the envisaged GDPR, was being discussed, the Council of Europe also decided to modernise Convention 108 "in order to better address emerging privacy challenges resulting from the increasing use of new information and communication technologies (IT), the globalisation of processing operations and the ever greater flows of personal data, and, at the same time, to strengthen the Convention's evaluation and follow-up mechanism".[11] The modernised convention is now referred to as **"Convention 108+"** and was adopted during the 128th session of the Committee of Ministers, on 18 May 2018. It was not the ambition of the Council of Europe to adopt a regional convention. Since its adoption, the Council of Europe has been seeking to transform 'Convention 108+' into a global convention, promoting accession by countries outside Europe. Since then, in addition to the 47 European participating states, eight countries outside Europe have become parties, including: Uruguay, Mauritius, Senegal, Tunisia, Cape Verde, Mexico, Argentina and Morocco, with further outreach to Burkina Faso.[12]

---

[6] See for the full text: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[7] See for the full text: http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

[8] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[9] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Strasbourg, 28 January 28, 1981, ETS no 108).

[10] It has been, moreover, ratified by countries outside the Council of Europe. See: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=mScbc290.

[11] Explanatory Memorandum, to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Series nr. 223.

[12] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures; Greenleaf, Graham and Cottier, Bertil, Comparing African Data Privacy Laws: International, African and Regional Commitments (April 22, 2020). University of New South Wales Law Research Series, 2020, Available at SSRN: https://ssrn.com/abstract=3582478

1.2. A strong fundamental rights foundation – coherent systems

It is important, with a view to give a legal assessment of data protection approaches, to emphasise the human rights dimension of data protection. Various international documents make reference to it.

> "It is important to emphasise the human rights dimension of data protection."

Within the **United Nations** to the right to privacy is referred to in its International Bill of Rights. The right to privacy is guaranteed by Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. Most regions in the world would now also recognize the right to privacy and/or data protection. The most important **European** instruments context are the European Convention on Human Rights (ECHR) and the Charter on Fundamental Rights of the European Union (CFREU). Article 8 of the ECHR guarantees the right to respect for private and family life. Articles 7 and 8 CFREU guarantee the right to private life and the right to data protection respectively. The Explanations on these articles of the CFREU provide that the rights guaranteed in this article correspond to those guaranteed by the ECHR. There is a vast area of case law of the European Court on Human Rights (ECtHR) with respect to Article 8 ECHR.

There are different important implications of surrounding the existence of, and embedding of rights within, fundamental rights frameworks. First of all, in principle everyone enjoys fundamental rights. It implies that also workers, but also organisations, including trade unions or private companies, may rely on fundamental rights protection. Secondly, no fundamental right is absolute. The enjoyment of fundamental rights can be subject to limitations. The relevance is that those limitations would need to be subject to the fundamental rights mechanism of protection, requiring a sufficient legal basis, a legitimate aim and a proportionate limitation. It would, nevertheless, mean that the exercise and protection of fundamental rights may be limited and balanced against other rights and interests. Fundamental rights are legal obstacles, but never in an absolute way. Likewise, the right to the protection of personal data is not an absolute right but needs to be considered in relation to its broader function in society.[13]

> "The exercise and protection of fundamental rights may be limited and balanced against other rights and interests. Fundamental rights are legal obstacles, but never in an absolute way."

A third important implication is that fundamental rights systems are coherent systems. This means that different fundamental rights may stand at the same legal level and the protection of multiple or different fundamental rights will need to be done in a coherent manner. In the context of this analysis, it is therefore important to stress that there may also be a fundamental rights nature of potentially opposing rights to the right to data protection, such as the fundamental right to collective bargaining or the right to information and consultation. It then would be important to make a proper realisation of the different rights at stake.

[13] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 6-7.

Different fundamental rights have already been opposed to the right to privacy and data protection. For example, Article 10 of the ECHR guarantees the right to freedom of expression also protects the free flow of information, which may oppose the right to data protection. Similarly, Article 11 of the ECHR guarantees the right to freedom of peaceful assembly and to freedom of association with others. This right includes the right to form and to join trade unions for the protection of the interests of individuals and the right to collective bargaining. Article 27 of the CFREU guarantees workers' right to information and consultation within the undertaking. Article 28 of the CFREU guarantees the right of collective bargaining and action, which includes the right to negotiate and conclude collective agreements and to take collective action to defend their interests. It is thus obvious that a clash between the right to data protection and the right to collective bargaining cannot only be solved through the data protection perspective.

"A clash between the right to data protection and the right to collective bargaining cannot only be solved through the data protection perspective".

1.3. Specific guidance for data protection in the work environment

While data protection instruments are in principle applicable in the employment context, various initiatives have been taken to create more specific guidance for the work environment. Some authoritative sources have to be taken into account in an assessment of data protection rules in light of the employment context.

- **ILO**: Due to the need to develop data protection principles that specifically address the use of workers' personal data, the ILO developed a Code of Practice. The ILO Code of Practice concerning the protection of workers' personal data was adopted by a Meeting of Experts on Workers' Privacy of the ILO in 1996.[14] The Preamble of the Code points out that the purpose is to provide guidance on the protection of workers' personal data. It has not been adopted as an ILO Convention or a Recommendation and does not have binding force. It is not designed to replace national laws, regulations, or international labour standards or other accepted standards. It should be used in the development of legislation, regulations, collective bargaining agreements, work regulations, policies and other practical measures.

- **EU Working Party**: Under the (former) 1995 European Data Protection Directive, the European 'Data Protection Working Party' adopted some guidance on data protection in the employment context. The Working Party'[15] adopted Opinion 8/2001 of 13 September 2001 on the processing of personal data in the employment context.[16] Another instrument is the EU Working Document of 29 May 2002 on workplace communications.[17] On 8 June 2017, the Working Party issued Opinion 2/2017 on data processing at work (WP Opinion 2/2017). It made a new assessment of issues "by outlining the risks posed by new technologies and

[14] ILO, *Protection of workers' personal data, An ILO code of practice*, 47 (1997).

[15] The Working Party is an advisory group composed by representatives of the data protection authorities of the Member States, which acts independently and has the task, inter alia, of examining any question covering the application of the national measures adopted under the Data Protection Directive in order to contribute to the uniform application of such measures.

[16] Opinion 8/2001 of 13 September 2001 on the processing of personal data in the employment context, 5062/01/EN/Final, WP 48, 28 p; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf .

[17] Data Protection Working Party, *Working Document on the Surveillance of Electronic Communications in the Workplace*, May 29, 2002, 5401/01/EN/final, 35 p.

undertaking a proportionality assessment of a number of scenarios in which they could be deployed".[18] Under the GDPR and its new governance model, the role of the Working Party's opinions remain authoritative and relevant.

- **Council of Europe Recommendation**: The desirability of adapting these data protection principles to the particular requirements of the employment sector led to the adoption of Recommendation No. R(89)2 on the Protection of Personal Data Used for Employment Purposes. This Recommendation was adopted by the Committee of Ministers on 18 January 1989 at the 423rd meeting of the Ministers Deputies. On 1 April 2015, the Committee of Ministers adopted a new Recommendation on the processing of personal data in the employment context (CM/Rec(2015)5) at the 1224th meeting of the Ministers' Deputies.[19] This revised recommendation was motivated due to "the changes which have occurred internationally in the employment sector and related activities, notably due to the increased use of information and communication technologies (ICTs) and the globalisation of employment and services".[20]

1.4. Key findings

- ✓ The GDPR is not an isolated instrument, though it is an essential and binding instrument in EU law, with an important influence and effect outside the EU.

*

- ✓ Data protection standards rely on fundamental rights frameworks.
- ✓ It may be necessary to reconcile different fundamental rights, as there is no general system of preference between these fundamental rights.
- ✓ This increases the importance of *framing* the rights conflicts involved

*

- ✓ The GDPR is a general instrument, applying to a wide field of activities with a broad scope of application.
- ✓ It is necessary to adapt the rules and principles of the GDPR – like all general data protection standards – to the specificities of the employment context.

[18] See: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.
[19] https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a.
[20] See the preamble of Recommendation CM/Rec(2015)5.

Chapter 2. Data protection standards and information rights

This chapter sets the broader narrative and fundamental rights framework and deals with the fundamental conflict between information rights and the right to data protection. It is important to define the relationship between data protection standards and the freedom of information and to establish a narrative for the relation between the GDPR and industrial relations. The right to information (connected with consultations and negotiations) is a collective labour right, not a stand-alone right in the context of data protection. It must be pointed out that, in principle, the GDPR is also based on the free flow of information principle. This foundation may prove to be important as both data protection and free information are fundamental rights. In that context, it is also relevant to position the concept of confidentiality as a limit to free information, and/or as part of data protection, in terms of scope and limits.

2.1. Foundations data protection standards

As this study aims to appreciate the right to information and collective bargaining in an employment and industrial relations context, it is highly relevant to indicate how data protection standards and the idea of information rights and freedom are related. The foundations and origins of data protection standards rather confirm than contradict information rights.

The development of standards in this field go hand in hand with the development of information and communication technologies.[21] Technological progress should therefore be considered as one of the main drivers for data protection standards. This is also stressed in the GDPR.[22] It is obvious that technology enhances the (free) flow of personal data, also in terms of higher processing speed and lower costs.[23]

It is important to understand this context, as data protection law does not necessarily contradict the increasing needs for information flows. On the contrary, regulating flows of data is part of a strategy to allow information to circulate freely.[24] In this context, the concept of 'data protection' might even be misleading, as these standards do not protect data as such, but rather the rights of persons whose personal data is being processed.[25] The point is thus to regulate data processing and technology and to establish rules that respond to fundamental rights of individuals. In their origin, data protection principles must be understood as not really opposing rights to information, but rather structuring and regulating it.

> "Data protection principles must be understood as not really opposing rights to information, but rather structuring and regulating it".

It is in light of this that modernized Convention no. 108 emphasizes the importance of personal autonomy based on the individual right to control personal data and the processing of these data.[26] From this perspective, data protection standards assume a role in regulating the 'information power balance'.

[21] D. KORFF & M. GEORGES, The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, 11.
[22] Consid. 6 Preamble GDPR.
[23] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, convention no. 108, 28 January 1981, 1.
[24] C. KUNER, *Transborder Data Flows and Data Privacy Law*, Oxford, Oxford University Press, 2013, 158.
[25] D. KORFF & M. GEORGES, The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, 12.
[26] Preamble Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data.

As confirmed in different instruments, the fact that natural persons should have control of their own personal data[27] should not be overlooked.[28] In that regard, the explanatory report of Convention no. 108 states that automatic data protection is concerned with "information power", as decisions on individuals are based on information in computerized data files (such as payroll data).[29] This could lead to a weakening of the position of these individuals, or – translated to the employment context – of workers. This "major objective" is repeated in the explanatory report of the modernized Convention:

> "*A major objective of the Convention is to put individuals in a position to know about, to understand and to control the processing of their personal data by others. Accordingly, the preamble expressly refers to the right to personal autonomy and the right to control one's personal data, which stems in particular from the right to privacy, as well as to the dignity of individuals. Human dignity requires that safeguards be put in place when processing personal data, in order for individuals not to be treated as mere objects*".[30]

This enhanced control over personal information and its role in data protection law is demonstrated through the rights-based approach in data protection standards (such as the right to access to data or the right to be informed in the GDPR).[31] The approach of regulating the 'information power balance' is of course also interesting and relevant for the industrial relations context. Labour laws are also part of the legal mechanisms to regulate power imbalances. Put otherwise, in regulating information power imbalances, both data protection and labour rights may be seen to have similar foundations and aims. In addition to this, the interconnection between labour rights and data protection rights would be too narrow when the view on data protection standards would be seen only as mere instruments to achieve personal autonomy. This may emphasize too much the individual freedom aspect and not enough the wider societal interests.[32] Data protection standards are considered as part of a system of checks and balances.[33] Hence, data protection standards may be observed as a means to strike a fair balance between the interests or power of data controllers and the autonomy or control of data subjects of their personal data.

"In regulating information power imbalances, both data protection and labour rights may be seen to have similar foundations and aims. Data protection standards are part of a system of checks and balances."

2.2. The market function of personal data standards

Freedom of information lies at the origin of (international) data protection standards. Within the EU, the relationship between free flow of information, data protection and the internal market has well been established both in the original Data Protection Directive and in the jurisprudence of the Court

[27] Consid. 7 Preamble GDPR.
[28] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, convention no. 108, 28 January 1981, 2.
[29] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, convention no. 108, 28 January 1981, 1.
[30] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, 2.
[31] O. LYNSKEY, The foundations of EU Data Protection Law, Oxford, Oxford University Press, 2015, 11.
[32] D. KORFF & M. GEORGES, The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, 13.
[33] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS and COUNCIL OF EUROPE, *Handbook on European data protection law*, Luxembourg: Publications Office of the European Union, 2018, 19.

of Justice of the European Union (CJEU).[34] The CJEU recognized that EU data protection law[35] was "*intended to ensure the free movement of personal data between Member States through the harmonisation of national provisions on the protection of individuals with regard to the processing of such data*".[36] It would imply that the transnational flow of personal data thus supports the internal market freedoms of businesses. In other words, a high level of data protection is considered as a *conditio sine qua non* for the free flow of personal data in the internal market of the EU.[37]

The fact that data protection standards are seen as a function of the internal market, has given the free movement of personal data the label as a 'fifth' market freedom, allowing transfers of personal data that would promote cross-border business activities.[38] The internal market function is significant.[39] As the Commission explained in a Communication, the free flow of personal data is necessary for the internal market which *requires that personal data be transferable between business people involved In cross-border activities*".[40]

Some nuance has to be made, while the market function has been strengthened. The GDPR has a different legal basis than the original Data Protection Directive. The preamble of the GDPR refers to article 16 TFEU. This article falls within the section of the general provisions of the Treaty and not within the section of the internal market. Although this article emphasizes the right to the protection of personal data, it still refers to the rules relating to the free movement of personal data and is building further on the idea of the internal market.[41] The explanatory memorandum of the GDPR confirms the free movement of personal data[42] and recalls that the Regulation will improve the protection of the fundamental rights as well as contribute to the functioning of the internal market.[43] In light of the 'market function', preventing restrictions or prohibitions on the free movement of personal data is still mentioned as one of the objectives in the GDPR.[44] In *Rechnungshof v. Österreichischer Rundfunk and others*, the CJEU the function of the internal market as an "*essential objective*" underlying data protection law.[45]

"In light of the 'market function', preventing restrictions or prohibitions on the free movement of personal data is mentioned as one of the objectives in the GDPR."

International and European data protection standards, developed outside the EU, pursue similar objectives. One of the main drivers behind Convention no. 108 of the Council of Europe was the fear

[34] Art. 1 Data Protection Directive.
[35] CJEU 20 May 2003, Rechnungshof / Österreichischer Rundfunk and others, C-465/00, §39.
[36] Ibid.
[37] D. KORFF & M. GEORGES, The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, 25.
[38] W. Gregory Voss. Cross-Border Data Flows, the GDPR, and Data Governance (29 Wash. Int'l L.J. 485 (2020). Washington International Law Journal, University of Washington, School of Law / Washington International Law Journal Association, 2020, 29 (3), 504.
[39] O. LYNSKEY, The foundations of EU Data Protection Law, Oxford, Oxford University Press, 2015, 49-50.
[40] COMMISSION COMMUNICATION on the protection of Individuals In relation to the processing of personal data In the Community and Information security, COM(90) 314, 16.
[41] Art. 16 TFEU
[42] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM (2012) 11, 5.
[43] Ibid, 5-6.
[44] Art. 1, 3 GDPR.
[45] CJEU 20 May 2003, Rechnungshof / Österreichischer Rundfunk and others, C-465/00, §42.

of national privacy laws became barriers to the free flow of information.[46] The modernized Convention no. 108 also recognizes "*that it is necessary to promote at the global level the fundamental values of respect for privacy and protection of personal data, thereby contributing to the free flow of information between people*".[47] Similarly, the OECD guidelines on data protection recognize "*that transborder flows of personal data contribute to economic and social development*" and "*that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows*".[48] That is why these guidelines aim at advancing the free flow of information between member countries and avoiding the creation of unjustified obstacles to the development of economic and social relations among Member countries.[49] In seeing freedom of information and data as part of the goals of data protection instruments, free flow of data is seen as essential to safeguard human rights and fundamental freedoms.[50] One may, for example, think about the right to information in the industrial relations context. Another consequence is, as the OECD has pointed out, that data protection standards "*ensure that the spread of privacy laws should not unduly restrict transborder data flows and the economic and social benefits they bring*".[51]

"In seeing freedom of information and data as part of the goals of data protection, free flow of data is seen as essential to safeguard human rights, for example in the industrial relations context."

2.3. Freedom of information as a fundamental right

As data protection standards regulate data flows, the freedom of information becomes an important dimension in appreciating possible conflicts of rights.

A major European source of the freedom of information as a fundamental right is article 10 ECHR, which entails the fundamental freedom of expression. This right to freedom of expression also contains the right to receive and impart information. Whereas data protection standards support the free flow of information, they can also see to support the right to receive information.

"Whereas data protection standards support the free flow of information, they can also see to support the right to receive information"

The European Court of Human Rights confirmed in several cases that article 10 ECHR is applicable in "*the relations between employer and employee are governed* […] *by private law, and that the State has a positive obligation to protect the right to freedom of expression even in the sphere of relations between individuals*".[52] While this case law has not yet been applied in the context of the right to receive or to impart information in an employment context, the case law has nevertheless protected the freedom

[46] B. VAN ALSENOY, *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 225.
[47] Preamble Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data.
[48] Preamble OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
[49] Ibid.
[50] Ibid.
[51] The evolving privacy landscape: 30 years after the oecd privacy guidelines, The OECD Privacy framework, 2013, 67.
[52] ECtHR 5 November 2019, no. 11608/15, HERBAI v. HUNGARY, § 37.

to receive information on the basis of article 10 ECHR and, as such, opposing it to privacy and data protection.

Cases in which the right to respect for private life (art. 8 ECHR) conflicts with the right to freedom of expression (and freedom of information) are most frequently handled in light of the protection of someone's reputation or the right to privacy of other people in the context of disclosing intimate information about one's private life. In the context of the employment relationship various cases deal with the protection of whistle-blowing. In other words, these cases are concerned with limiting the workers' right to disclose information and make the information publicly.

Mostly, the ECtHR's case law would make a broad balance of rights and interest. It is clear that a reconciliation may need to be made between the right of the employer (for example the right to confidentiality of commercial information[53] or the right to loyalty[54]) and the rights of workers or the broader public, or alternatively, between the right to privacy and the right to information.

This does not take away that the right to receive information is under development. In the case of *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung v. Austria*, the Court moved towards a broader interpretation of the notion of "freedom to receive information", acknowledging a right of access to information. As refusal of access to documents held was seen as an interference with the right under Article 10 ECHR. Another significant case is *Youth Initiative for Human Rights v. Serbia*. In that judgment, the Court stressed once again that "freedom to receive information" includes the right of access to information.[55]

2.4. Conflict of fundamental rights

The industrial relations examples of this report have the potential to raise a conflict between several fundamental rights. In essence, these examples deal with workers' representatives asking to receive information to employers that might entail personal data on workers. If the right to data protection is opposed to the right to information, the question is how the conflict between those two fundamental rights is solved. This depends on the perspective that is taken to identify which fundamental rights are triggered in this context.

"If the right to data protection is opposed to the right to information, the question is how the conflict between those two fundamental rights is solved. This depends on the perspective that is taken to identify which fundamental rights are triggered in this context."

The conflict of data protection rights with information rights is not new. As mentioned above, the right to receive information (as part of the freedom to expression) might interfere with the right to data protection (as part of the right to respect for private life). Other examples, for instance in collective bargaining, may demonstrate a potential conflict between the freedom of association and the right to privacy. Also, several other fundamental rights, provided in the Charter of Fundamental Rights of the European Union (CFREU), may be conflicting with the right to privacy (art. 7 CFREU) and data protection (art. 8 CFREU). The CFREU explicitly recognizes the workers' right to information and consultation with the undertaking

[53] Council of Europe/ European Court of Human Rights, *Guide on Article 10 of the European Convention on Human Rights*,2021, https://www.echr.coe.int/documents/guide_art_10_eng.pdf , 63; ECtHR 5 November 2019, no. 11608/15, Herbai v. Hungary, §§ 41-43.

[54] ECtHR 12 February 2008, no. 14277/04, Guja v. Moldova, § 70.

[55] D. BYCHAWSKA-SINIARSKA, *Protecting the right to freedom of expression under the European Convention on Human Rights*, Strasbourg, Council of Europe, 2017, 15.

(art. 27), the right of collective bargaining and action (art. 28) and the freedom to conduct a business (art. 16).

In short, many fundamental rights may be conflicting. Which specific fundamental rights will be in conflict, will depend from the "framing" of the examples. This makes it difficult to predict the outcome of this conflict. For this reason it will be necessary to apply an open and fundamental approach to these potential conflicts of rights.

Firstly, a theoretical approach will follow on how the Court of Human Rights deals with conflicts of human rights. Secondly, criteria are developed to deal with conflicts between two specific human rights based on the case law of the European Court of Human Rights. It is useful to examine how these fundamental rights are related with each other, considering the objective of the GDPR to protect *"fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".*[56] In other words, the purpose of the GDPR is mainly to establish the criteria and the conditions in order to achieve fair and lawful processing of personal data.

The approach of the European Court of Human Rights in order to analyze a human rights claim has a step-by-step nature: 1) does the complaint fall withing the scope of the relevant human right and, if so, does the applicant has suffered a detriment? 2) is this interference justified under the limitation clause of the relevant article?.[57] Regarding the conflicts of human rights, the case law of the European Court of Human Rights oscillates between two key principles.[58] It considers the constant search for a balance between fundamental rights of each individual as the foundation of a democratic society.[59] However, in its case law the ECtHR also states that the ECHR has to be read as a whole and interpreted in such a way to promote internal consistence between the provisions. [60]

This search for a fair balance may entail weighing up two rights of equal status.[61] Therefore, the European Court of Human Rights adopts a "balancing" method when two fundamental rights of articles 8-11 ECHR are in conflict with each other. This method entails weighing and balancing human rights and one protected interest or set of interest against another.[62] This balancing method has an open ended and ad hoc nature, because the Court weighs the interests in the circumstances of the case at hand.[63] This open ended balancing method allow the Court to decide freely which criteria it will apply in specific cases.[64] However, in some conflicts of two specific human rights the Court has established a non-exhaustive list of applicable criteria in order to resolve these conflicts. For instance, the Court developed a list of criteria in cases in which the right to freedom of expression and the right to respect for private life clash.[65]

---

[56] Art. 1.2 GDPR.

[57] S. SMET, *Resolving Conflicts between Human Rights: The judge's dilemma*, New York, Routledge, 2017, 23-24.

[58] Ibid, 18.

[59] ECtHR 29 April 1999,nos. 25088/94, 28331/95 and 28443/95, Chassagnou and Others v France, § 113.

[60] See, for instance, ECtHR 20 September 1994, no. 13470/87, Otto-Preminger-Institut v Austria, § 47; ECtHR 29 April 2002, no. 2346/02, Pretty v the United Kingdom, § 54.

[61] COUNCIL OF EUROPE/ EUROPEAN COURT OF HUMAN RIGHTS, *Guide on Article 10 of the European Convention on Human Rights*,2021, https://www.echr.coe.int/documents/guide_art_10_eng.pdf , 25 (under reference to ECtHR 7 February 2012, no. 39954/08, Von Hannover Case and Axel Springer).

[62] S. BESSON, *Human Rights in Relation: A Critical Reading of the ECtHR's Approach to Conflicts of Rights*, Oxford, Oxford University Press, 2017, 30.

[63] S. SMET, *Conflicts between Human Rights and the ECtHR: Towards a Structured Balancing Test*, Oxford, Oxford University Press, 2017, 39.

[64] Ibid, 40.

[65] COUNCIL OF EUROPE/ EUROPEAN COURT OF HUMAN RIGHTS, *Guide on Article 10 of the European Convention on Human Rights*, 28.

This method is derived from the 'necessary in a democratic society' test for the protection of the rights and freedoms of others, which is mentioned in all articles of the European Convention on Human Rights relevant for the examples in the first section of this report (art. 8-11 ECHR).[66]

The importance of framing the examples mentioned in the first section of this report is also shown by this approach of the European Court. The general principle of the European Court is that the ECHR is first and foremost a system for the protection of human rights and therefore justified restrictions have to be considered the exception.[67] This means that the proportionality test might entail the priority of the right invoked by the applicant over the interest put forward by the defending state to justify the restriction.[68] This may lead to framing the case around the directly invoked human right by the European Court, while disregarding the importance of the other human right.[69]

2.5. Information rights in industrial relations

Due to the need for balancing and identifying information rights at equal fundamental level of data protection rights, we elaborate our analysis with an information rights perspective in industrial relations.

Two major perspectives for information rights in industrial relations play a role: on the one hand, there is the fundamental right to information and consultation through workers' representatives; on the other hand there is the right to collective bargaining, which may entail information rights as well.

"Two major perspectives for information rights in industrial relations play a role: the right to information and consultation through workers' representatives; and the right to collective bargaining."

a. Sources on information and consultation

A number of important legal sources are relevant for the recognition of information rights in industrial relations.

- **The Charter of Fundamental Rights of the European Union recognizes the right to information and consultation within the undertaking:**

"*Workers or their representatives must, at the appropriate levels, be guaranteed information and consultation in good time in the cases and under the conditions provided for by Union law and national laws and practices*".[70]

The right to information and consultation is recognized as a fundamental right in the EU. This article applies under the conditions laid down by European or national law. The reference to the appropriate levels also refers to the levels laid down by European or national legislation.[71] This suggests that this fundamental right depends entirely upon European and national legal instruments.[72] In this regard the

[66] S. BESSON, *Human Rights in Relation: A Critical Reading of the ECtHR's Approach to Conflicts of Rights*, 34.
[67] S. SMET, *Resolving Conflicts between Human Rights: The judge's dilemma*, New York, Routledge, 2017, 33.
[68] S. SMET, *Resolving Conflicts between Human Rights: The judge's dilemma*, New York, Routledge, 2017, 35 under reference to O. De Schutter and F. Tulkens, 'Rights in Conflict: The European Court of Human Rights as a Pragmatic Institution', in E. Brems (ed.), *Conflicts between Fundamental Rights,* Antwerp, Intersentia, 2008, 188–190.
[69] S. SMET, Resolving Conflicts between Human Rights: The judge's dilemma, New York, Routledge, 2017, 36.
[70] Art. 27 CFREU.
[71] Explanations relating to the Charter Of Fundamental Rights, *OJ C* 303, 14 December 2007, 26.
[72] B. RYAN, "The Charter and Collective Labour Law" in T. Hervey and J. Kenner (eds.), *Economic and Social Rights under the EU Charter of Fundamental Rights—A Legal Perspective*, Oxford, Hart Publishing, 2003, 73.

explanations on the CFREU refer to "*Articles 154 and 155 of the Treaty on the Functioning of the European Union, and Directives 2002/14/EC (general framework for informing and consulting employees in the European Community), 98/59/EC (collective redundancies), 2001/23/EC (transfers of undertakings) and 94/45/EC (European works councils)*".[73] This provision does not impose new obligations to Member States, because the provision of the CFREU are addressed to the Member States "*only when they are implementing Union law*".[74] Therefore, the European Court of Justice ruled that in order to be fully effective, article 27 must be given "*more specific expression in European Union or national law*".[75]

The right to information and consultation is recognized as a fundamental right in the EU. It applies under the conditions laid down by European or national law.

Recognition as a fundamental right means it may only be limited if this is *necessary* to protect the rights and freedoms of others.

Recognition as a fundamental right also means that, on article 52 CFREU, the right to information and consultation in article 27 CFREU may only be limited if the limitation is provided by law and is necessary and responds to the need to protect the rights and freedoms of others (proportionality).[76]

- **The right to information and consultation is also mentioned in article 21 of the (revised) European Social Charter of the Council of Europe.**

The European Committee of Social Rights clarified that employees and/or their representatives have to be informed "of any matter that could affect their working environment, unless the disclosure of such information could be prejudicial to the undertaking. They must also be consulted in good time on proposed decisions that could substantially affect their interests, particularly ones that might have a significant impact on the employment situation in their undertaking".[77]

- **In 2002 the European Parliament and the Council adopted a Directive establishing a general framework for informing and consulting employees in the European Community.**

This directive provides a definition of information and consultation. On the one hand information means "*transmission by the employer to the employees' representatives of data in order to enable them to acquaint themselves with the subject matter and to examine it*".[78] On the other hand the directive defines consultation "*the exchange of views and establishment of dialogue between the employees' representatives and the employer*".[79] The directive refers to a list of types of information that are covered.

[73] Explanations relating to the Charter Of Fundamental Rights, *OJ C* 303, 14 December 2007, 26.
[74] Art. 51.1 CFREU.
[75] CJEU 15 January 2014, no. C-176-12, Association de médiation sociale v Union locale des syndicats CGT and Others, § 45.
[76] Art. 52 CFREU.
[77] EUROPEAN COMMITTEE OF SOCIAL RIGHTS, Digest of the case law of the European Committee of Social Rights, https://rm.coe.int/digest-2018-parts-i-ii-iii-iv-en/1680939f80 , 196. (under reference to Conclusions 2010, Belgium).
[78] Art. 2, F Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community, OJ L 080 ,23 March 2002 P. 0029 – 0034.
[79] Art. 2, G Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community, OJ L 080 , 23 March 2002 P. 0029 – 0034.

- **The European Works Council Directive also provides information and consultation rights to employees' representatives.**

The general purpose of this directive is "*to improve the right to information and to consultation of employees in Community-scale undertakings and Community-scale groups of undertakings*".[80] The competence of the European Works Council and the scope of the information and consultation procedures is limited to transnational issues.[81] In the directive the concept 'information' is defined rather broadly. It refers to the "*transmission of data by the employer to the employees' representatives in order to enable them to acquaint themselves with the subject matter and to examine it; information shall be given at such time, in such fashion and with such content as are appropriate to enable employees' representatives to undertake an in-depth assessment of the possible impact and, where appropriate, prepare for consultations with the competent organ of the Community-scale undertaking or Community-scale group of undertakings*".[82] There is no specific list of information that has to communicated to the EWC. The scope and functions of the EWC will be determined by written agreement negotiated between the central management and the special negotiating body.[83] The directive provides only a specific list of information regarding the competence of the EWC when the subsidiary requirements apply[84]. In these cases the "*information of the European Works Council shall relate in particular to the structure, economic and financial situation, probable development and production and sales of the Community-scale undertaking or group of undertakings. The information and consultation of the European Works Council shall relate in particular to the situation and probable trend of employment, investments, and substantial changes concerning organisation, introduction of new working methods or production processes, transfers of production, mergers, cut-backs or closures of undertakings, establishments or important parts thereof, and collective redundancies*".[85]

"There is no specific list of information that has to communicated to the EWC. The scope and functions of the EWC will be determined by written agreement negotiated between the central management and the special negotiating body."

The **directives on collective dismissal and transfer of undertakings** do not mention a definition on information. However, these directives provide a fixed list of certain types of information that has to be supplied to the workers' representatives.

Some countries provide a specific list of information that has to be given to committees of workers in enterprises. For instance, in France the Code du travail states that the "Comité social et économique" has to be informed annually on, among others, the implementation of professional interviews, working hours (overtime worked within and beyond the annual quota, part-time work, the duration and organization of working time, the period for taking paid leave and the procedures for monitoring the workload of the employees concerned), the measures taken to facilitate the employment of workers

[80] Art. 1.1 Directive 2009/38/EC of the European Parliament and of the Council of 6 May 2009 on the establishment of a European Works Council or a procedure in Community-scale undertakings and Community-scale groups of undertakings for the purposes of informing and consulting employees OJ L 122, 16.5.2009, p. 28–44 (Hereinafter: EWC Directive).
[81] Art. 1.3 EWC Directive.
[82] Art. 2.1, f EWC Directive.
[83] Art. 5.3 and art. 6.2, c EWC Directive.
[84] Art. 7.1 EWC Directive.
[85] Annex I EWC Directive.

injured in work and information relating to the provision contracts conclude with temporary employment companies.[86]

b. Sources on collective bargaining

The **Charter of Fundamental Rights of the European Union** recognizes the right of collective bargaining (article 28). The right to collective bargaining is also mentioned in article 6 of the **European Social Charter** of the Council of Europe.

The provisions are rather open textured. The European Committee of Social Rights noted that "*participation requires, as a prerequisite, exchange of information and consultation between employers and workers, as provided for under paragraph 1 of Article 6*".[87] The article does not provide a right to consultation. It is an obligation of the State to promote the consultation.[88] But it has been accepted that joint consultation implies information and is a precondition of an effective collective bargaining.[89] It means that if employers and trade unions enter into consultations or negotiations, information exchange can be seen as a condition for effective bargaining.

If employers and trade unions enter into consultations or negotiations, information exchange can be seen as a condition for effective bargaining. Some legal instruments point at the necessity to give information in bargaining processes.

It cannot be ignored that providing information is essential for collective bargaining processes.[90] Therefore, some legal instruments point at the necessity to give information in bargaining processes. This is also recognized in the Collective Bargaining Recommendation no. 163 of the ILO:

> "*employers should, at the request of workers' organisations, make available such information on the economic and social situation of the negotiating unit and the undertaking as a whole, as is necessary for meaningful negotiations*".[91]

The ILO Declaration concerning Multinational Enterprises and Social Policy also requires that workers' representatives receive information in order to establish meaningful negotiations.[92]

In context of the (former) **European Works Council Directive**, the CJEU emphasised explicitly the importance of access to information in light of collective negotiations: "*if the Directive is to serve a useful purpose, it is essential that the employees concerned be guaranteed access to information enabling them to determine whether they have the right to demand the opening of negotiations between central management and the employees' representatives, such a right to information constituting a necessary prerequisite for determining whether a Community-scale undertaking or group of undertakings exists, which is itself a condition precedent for the setting up of a European Works*

[86] Article L2312-26 Code du travail.
[87] EUROPEAN COMMITTEE OF SOCIAL RIGHTS, Conclusions VII (Art. 6-1- Joint consultation, 1981, 35; R. BIRK, "The Rights Guaranteed by the Social Charter" in R. BLANPAIN (ed.), *International Encyclopaedia for Labour Law and Industrial Relations,* Mechelen, Wolters Kluwer, 2007, 339.
[88] Ibid, 339.
[89] Ibid, 339.
[90] J. PEETERS, *Informatie en raadpleging van werknemers bij herstructurering,* Antwerp-Oxford, 2009, 71.
[91] Art. 7 Recommendation no. 163.
[92] INTERNATIONAL LABOUR ORGANISATION, Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy, https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emp_ent/---multi/documents/publication/wcms_094386.pdf , 14, no. 61.

Council or of a transnational procedure for informing and consulting employees".[93] In another case the CJEU mentioned a similar consideration: "*It also follows that, to the extent that it is necessary in order to make it possible for the employees concerned or their representatives to gain access to the information which is essential if they are to be able to determine whether or not they are entitled to request the opening of negotiations, communication of documents clarifying and explaining the information which is indispensable for that purpose may also be required, in so far as that communication is necessary*".[94]

In various systems, union delegates have information rights in light of consultation and bargaining. In France, for example, trade unions have well-established rights in light of collective bargaining. Each representative union may appoint one or several union delegates.[95] These delegates have specific information and consultation rights.

c. Confidentiality

Information rights may be limited by rules of confidentiality. In industrial relations laws, different references to this can be found.

- The **European Social Charter** provides explicitly that the disclosure of certain information which could be prejudicial to the undertaking may be refused or subject to confidentiality.[96]
- Article 6 of **Directive 2002/14** refers to confidential information in context of information and consultation. The directive does not exclude the right to receive information on the basis of confidentiality. However, It provides that Member States have to provide the conditions and limits laid down by national legislation to employees' representatives the authorization to reveal to employees information that has expressly been provided to them in confidence.[97] The Directive also allows that Member States provide specific cases (and conditions) in national legislation, in which the employer is not obliged to communicate information when the nature of that information would, according to objective criteria, "*seriously harm the functioning of the undertaking or establishment or would be prejudicial to it*".[98] Finally, Member States have to provide administrative or judicial review procedures for the case "*where the employer requires confidentiality or does not provide the information in accordance with paragraphs 1 and 2* [of article 6 of the Directive 2002/14]" and also "*procedures intended to safeguard the confidentiality of the information in question*".[99]
- In 2008 the European Commission published a working document on the review of the application of the Directive 2002/14/EC.[100] In this document there is an overview regarding the transposition in Member States of the notion 'confidentiality' in the Directive. The Commission notes in this comparative analysis that some Member States largely reproduce

[93] CJEU 13 January 2004, no. C-440/00, Gesamtbetriebsrat der Kühne & Nagel AG & Co. KG v Kühne & Nagel AG & Co. KG., § 46 under reference to CJEU 29 March 2001, no. C-62/99, Betriebsrat der bofrost Josef H. Boquoi Deutschland West GmbH & Co. KG v Bofrost* Josef H. Boquoi Deutschland West GmbH & Co. KG., § 32.
[94] CJEU 29 March 2001, no. C-62/99, Betriebsrat der bofrost Josef H. Boquoi Deutschland West GmbH & Co. KG v Bofrost* Josef H. Boquoi Deutschland West GmbH & Co. KG., § 40.
[95] M. DESPAX, J.-P. and J. ROJOT. 'France. In International Encyclopaedia of Laws: Labour Law and Industrial Relations, edited by Roger Blanpain. Alphen aan den Rijn, NL: Kluwer Law International, 2017, 296.
[96] Art. 21 European Social Charter.
[97] Art. 6.1 Directive 2002/14/EC.
[98] Art. 6.2 Directive 2002/14/EC.
[99] Art. 6.3 Directive 2002/14/EC.
[100] Commission staff working document accompanying the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the review of the application of Directive 2002/14/EC in the EU.

the definition of confidentiality provided in the directive. Other Member States transposed confidentiality in terms of "in the legitimate interest of the undertaking or establishment". Other Member States refer to the terms "commercial, industrial, business or professional secret" or the "possibility to cause harm or prejudice to the undertaking" in this regard. Some Member States merely use "information of a confidential character" without any specification. Finally, some Member States emphasize the confidentiality of specific information (e.g. on fabrication issues or the financial position and security). Some Member States require that the employer indicates which information is considered confidential or even justify the confidential nature of the information. In some Member States there is also a distinction between the obligation of secrecy and the obligation of discretion.

- The **European Works Council Directive** has a similar provision on confidentiality in context of information and consultation procedures.[101] The Directive protects confidential information in two ways: an obligation on the members of the European Works Councils not to divulge certain information defined as confidential by the central management and the right of the central management not to provide information in certain circumstances.[102] The Directive refers to national legislation to lay down the conditions and limits when the central management is not obliged to transmit confidential information by means of objective criteria.[103] However, it is rather unclear how these objective criteria will be defined. Therefore, Blanpain argues that the only criterion to allow employers not to meet his obligation to provide information is when the disclosure may "*seriously harm the functioning of the undertakings concerned or … be prejudicial to them*".[104]

The scope of confidential information, limiting information rights, is obviously subject to discussion. The texts of the European legislation would rather refer to harm to the undertaking. Some countries refer to the limits arising from "commercial, industrial, business or professional secrets". None of the examples give insight into whether personal data fall under confidential information as provided by industrial relations laws. In various cases, confidentiality will be subject to an agreement with the parties involved.

The scope of confidential information, limiting information rights, is obviously subject to discussion. None of the examples give insight into whether personal data fall under confidential information as provided by industrial relations laws.

To give some other examples, in Germany the notion of confidentiality in the Act on European Works Councils refers to business secrets in a technical sense and has been interpreted in a rather restrictive way by the courts.[105] Belgian law provides a list of specific information that would harm the functioning of the undertaking or would be prejudicial to it: "*information on the distribution margins; turnover in absolute terms and broken down per undertaking that is part of the group; level and trend in unit cost and selling prices per unit; data on cost distribution*

[101] Art. 8 DIRECTIVE 2009/38/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 May 2009 on the establishment of a European Works Council or a procedure in Community-scale undertakings and Community-scale groups of undertakings for the purposes of informing and consulting employees.
[102] IELL analysis directive 2009/38, 84.
[103] Art. 8.2 8 DIRECTIVE 2009/38/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 May 2009 on the establishment of a European Works Council or a procedure in Community-scale undertakings and Community-scale groups of undertakings for the purposes of informing and consulting employees
[104] R. BLANPAIN, 'Analysis of the European Directive 2009/38/EC of 6 May 2009' in F. HENDRICKX (ed.), IEL Labour Law, (Kluwer Law International BV, Netherlands: 2009), https://kluwerlawonline.com/EncyclopediaChapter/IEL+Labour+Law/IELL20190087, 85.
[105] E. HEIMANN, 'EWC: Germany', in F. HENDRICKX (ed.), IEL Labour Law, (Kluwer Law International BV, Netherlands: 2019), https://kluwerlawonline.com/EncyclopediaChapter/IEL+Labour+Law/IELL20190096, 24.

per product and per undertaking that is part of the group; under the heading of the program and general view of the future per undertakings in the distribution business: intentions regarding the opening of new sales outlets; data with regard to scientific research; the distribution by undertaking that is part of the group of profit and loss account data".[106] Italy adopted a very similar provision as the EWC Directive. It imposes confidentiality requirements on EWC representatives without further specification. The provision also states that the central management is not obliged to provide any information which would objectively and seriously harm the functioning of the undertakings concerned or would be prejudicial to them.[107] French legislation only imposes a professional secrecy on production proceeds on the members and experts in EWC. They have also the duty to keep confidential information designated by the employer as confidential.[108] However, like the Italian legislation, it does not clarifies which information may be subject to the confidentiality requirement.

Other directives on the information and consultation of workers do not mention the confidentiality of information. A possible reason may be the fixed list of information that has to be communicated to the workers' representatives in procedures of collective dismissal and transfer of undertakings.

2.6. Benchmark cases

Where in this chapter we are looking for reconciling data protection rights and information rights under a broad fundamental rights umbrella, we identify two benchmark cases that show the fact that data protection rules principles can (have to) be balanced against other, opposing, rights and interests. One example relates to the principle of equal pay. In order to effectively build up an equal pay, personal data of (other) workers may be required. Another example relates to personal data which may be given to workers representatives. The GDPR shows to be a context where data protection does not necessarily block all personal data disclosure and legitimate and proportionate responses may be offered to allow personal data disclosure to interested recipients.

a. Works council

Evidence of the interaction between the right to information and the protection of personal data is highly uncommon. In our research, one case in Germany handled on this particular interaction. It relates to a dispute concerning an airline company that had given pregnant employees the option that the employer would not inform the works council of their pregnancy.

The German Federal Labour Court (hereinafter: the Court), before which the case appeared, states that the request for information, from the representatives, is not a priori incompatible with the GDPR.[109] In terms of scope of application of the GDPR, the Court notes that the notification of an employee's pregnancy by name to the works council by the employer constitutes non-automated data processing on an identified natural person stored in a file system. The provision of information by transmission does not require that it be to a third party. Moreover, information about a pregnancy has

[106] C. ENGELS, 'EWC: Belgium', in F. HENDRICKX (ed.), IEL Labour Law, (Kluwer Law International BV, Netherlands: 2019), https://kluwerlawonline.com/EncyclopediaChapter/IEL+Labour+Law/IELL20190089, 63 under reference to Royal Decree in furtherance of Article 8 the Law laying down Accompanying Measures of 23 Apr. 1998, 10 Aug. 1998, Official Gazette 17 Oct. 1998.
[107] M. CAVALLINI, 'EWC: Italy', in F. HENDRICKX (ed.), IEL Labour Law, (Kluwer Law International BV, Netherlands: 2013), https://kluwerlawonline.com/EncyclopediaChapter/IEL+Labour+Law/IELL20190099, 31.
[108] S. CALME, 'EWC: France' in F. HENDRICKX (ed.), IEL Labour Law, (Kluwer Law International BV, Netherlands: 2021), https://kluwerlawonline.com/EncyclopediaChapter/IEL+Labour+Law/IELL20190095, 30.
[109] Bundesarbeidsgericht 9 April 2019, no. ARB 51/17, ECLI:DE:BAG:2019:090419.B.1ABR51.17.0, https://www.bundesarbeitsgericht.de.

to be considered health data Consequently, these data fall under the category of special data within the meaning of Article 9 GDPR.

Subsequently, the Court examines whether the right to information of the works council constitutes as legal obligation for employers and, therefore, whether this may provide a legal basis for this data processing. The Court mentions that the national legislation (and article 9 of the GDPR) provides that these data can be processed in the context of the employment relationship for the exercise of rights or the fulfilment of legal obligations under employment law. More specifically, the Court examines whether the works council is entitled to receive information about the pregnant employee based on a general legal obligation for employers "to supply comprehensive information to the works council in good time to enable it to discharge its duties under this Act", after the employer has been informed by the employee about the pregnancy. In this way, the Court aims to verify whether this data processing is necessary for the fulfilment of a legal obligation as an exception ground to allow this data processing. The criterion of the necessity of the data processing serves to ensure that the data are not processed excessively. In this case, this condition is met if the data processing is necessary for the fulfilment of a right arising from the law to protect the interests of employees. Here, the Court refers to the requirement to take appropriate and specific measures to protect the interests of employees. The Court then states that it must be shown that the information requested is indispensable to the performance of the task as a works council. The general right to information contained in a statutory provision can justify the necessity of personal data processing. According to the Court, this applies at least if the works council requests information to fulfil a legal obligation. The fact that the national statutory provision only provides for a general right to information does not detract from this.

> "The Court states that it must be shown that the information requested is indispensable to the performance of the task as a works council. The general right to information contained in a statutory provision can justify the necessity of personal data processing."

The Court then refers to the exception ground in Article 9 GDPR to process special data that requires to provide appropriate safeguards. In this regard, the works council must explain in the information request what measures will be taken to protect the legitimate interests of the employees concerned. This specific obligation applies to the works council regardless of whether the works council is part of the controller or is itself the controller. As part of the appropriate measures that the works council has to take in order to protect these personal data, it is required that there are guarantees for data subjects. The Court gives some examples, such as confidentiality, or securing and restricting access to the confidential data to the individual members of the works council and deleting these data when the monitoring task has been fulfilled. It is important that the works councils take these adequate measures. When they do not take sufficiently protective measures, the works councils cannot execute its information request.

> "It is required that there are guarantees for data subjects. The Court gives some examples, such as confidentiality, or securing and restricting access to the confidential data to the individual members of the works council and deleting these data when the monitoring task has been fulfilled".

Finally, the Court emphasizes that employees cannot object to this transfer of their data. Article 18 GDPR only provides a right to object when these data are processed under Article 6(1)(e) or (f) GDPR. In this case, the data are processed under Article 9(2)(b) GDPR.

b. Equal pay

On 4 March 2021, the European Commission made a proposal of a European Directive to strengthen the application of the principle of equal pay for equal work between men and women through pay transparency.[110] In the 30th Recital of this proposal, it is pointed out that "specific safeguards should be added *to prevent the direct or indirect disclosure of information of an identifiable co-worker*."[111]

Indeed, the proposal provides for a right for workers to receive information about pay levels in an organization. The right can be exercises through the workers' representatives. However, it not only applies to the own individual salary, but also to the average pay levels of other workers. According to article 7 of the proposal:

> "workers shall have the right to receive information on their individual pay level and the average pay levels, broken down by sex, for categories of workers doing the same work as them or work of equal value to theirs"

Employers may require that any worker having obtained such pay information, shall not use that information for any other purpose than to defend their right to equal pay and not disseminate the information otherwise.[112] Interestingly, the proposed directive also contains provisions on data protection. The question, indeed, arises as to what extent employers can disclose individual salary information of workers to workers' representatives or to other individual workers. It is clear from the proposed EU directive that, within the context of data protection, workers' representatives can receive personal data related to pay. Disclosing personal data to workers' representatives rather than to individual workers is seen as a solution, rather than a problem, in light of the GDPR.

There is, however, an additional safeguard in case information "would lead to the disclosure, either directly or indirectly, of the pay of an identifiable co-worker. Member States may decide that in such case, accessibility of the information shall be limited to the workers' representatives or to the equality body. These will advise the worker regarding a possible claim, without disclosing actual pay levels of individual workers doing the same work or work of equal value."[113]

"Member States may decide that accessibility of the information shall be limited to the workers' representatives or to the equality body. These will advise the worker regarding a possible claim, without disclosing actual pay levels of individual workers doing the same work or work of equal value."

It is clear that this is a sensitive issue. This is also clear from that fact that the European Data Protection Supervisor

[110] Proposal for a Directive of the European Parliament and of the Council to strengthen the application of the principle of equal pay for equal work or work of equal value between men and women through pay transparency and enforcement mechanisms, COM/2021/93 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0093.

[111] Our emphasis.

[112] Proposal for a Directive of the European Parliament and of the Council to strengthen the application of the principle of equal pay for equal work or work of equal value between men and women through pay transparency and enforcement mechanisms, COM/2021/93 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0093&from=EN.

[113] Proposal for a Directive of the European Parliament and of the Council to strengthen the application of the principle of equal pay for equal work or work of equal value between men and women through pay transparency and enforcement mechanisms, COM/2021/93 final, p14, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0093.

(EDPS) has given an opinion on this draft.[114] The EDPS has recommended that the issue of providing for specific safeguards to prevent disclosure of individual (personal) data, as expressed in the 30th Recital, mentioned above, would be integrated in the text of the final version of the proposed directive. It has, however, not suggested to delete the section on making workers' representatives recipients of such personal data, where this solution would be taken. On the contrary, overall, the EDPS concluded that the Commission's proposed directive does raise major data protection issues.

2.7. Key findings

- ✓ Data protection standards are not designed to *prohibit* data or information flows.
- ✓ The right to information and consultation is recognized as a fundamental right in Europe, subject to certain conditions.
- ✓ None of the examples studied give insight into whether personal data fall under confidential information as provided by industrial relations laws.

*

- ✓ Two benchmark cases show that data protection standards, such as the GDPR, do not stand in the way of disclosing personal data related to workers to the workers' representatives.
- ✓ A European legislative proposal on equal pay allows individual pay data to be shared with workers' representatives. Arrangements can be made whereby disclosure individual pay information will be limited to the workers' representatives, not to individual workers.
- ✓ A German case confirms that information rights of works council representatives can be reconciled with the GDPR, even if it concerns sensitive information.
- ✓ An important requirement is that it must be shown that the information requested is indispensable to the performance of the task as a works council (representative).
- ✓ The general right to information contained in a statutory provision can be a basis to justify the necessity of personal data processing (disclosure).

[114] Formal Comments of 27 April 2021, https://edps.europa.eu/system/files/2021-04/21-04-27_2021-0251_d0905_comments_en.pdf.

Chapter 3. HR and IR justifications under the GDPR framework

This chapter focuses on the GDPR and relates to how the major principles of data protection can support HR and IR personal data processing. In order to respond to the issues and problems set out in the introduction and problem analysis, it is relevant to give legitimacy and justification grounds for information and data exchange in the industrial relations context. It must be pointed out that the GDPR provisions are quite open textured and leave room for interpretations. They thus bear potential for the industrial relations context. In this chapter, we also show some benchmark cases where data protection standards and rights to information on HR personal data need to be reconciled.

3.1. Introduction

In light of the problem setting of the present study, data protection standards will play a key role in developing solutions for collection, further processing and disclosing of personal data in the context of HR and industrial relations. The data protection rules and principles will guide stakeholders with regard to personal data through various conditions and benchmarks. In view of this study, it is important to analyse three main and essential data protection principles which need to be considered:

- Legitimacy
- Proportionality
- Purpose limitation

Besides these key principles, we also pay attention to the right to access to personal data. This right is a typical component of data protection and has some features which are relevant for the employment context.

At the end of this chapter, we describe two benchmark cases that show the fact that data protection rules principles can (have to) be balanced against other, opposing, rights and interests. One example relates to the principle of equal pay. Another example relates to personal data which may be given to workers representatives.

3.2. Legitimacy

a. General

A general and essential requirement of data protection standards is that personal data must be collected and processed on a legitimate ground, reason or purpose. In other words, personal data processing has to be justified on the basis of a legitimate ground. A legitimate basis requires, above all, that it is lawful.

This principle of lawfulness or legitimacy stands central in data protection law and has been further specified in different data protection instruments around the globe. The principle is also confirmed by the European human rights framework, including article 8 of the EU Charter of Fundamental Rights.[115] It must be noted, furthermore, that this principle applies to all data processing, not only for collection of personal data, but

It must be noted, furthermore, that this principle applies to all data processing, not only for collection of personal data, but also for further processing, including disclosure or communication of data to third parties.

[115] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS and COUNCIL OF EUROPE, Handbook on European data protection law, 19.

also for further processing, including disclosure or communication of data to third parties.

The evaluation of this legitimacy principle will be dependent on the context and circumstances of data processing. In light of this, the employment relationship is generally recognised as a legitimate basis for personal data processing under data protection law. Obviously, the link with the employment relationship should be established in a proper way.

While the (employment) contract may be a strong and legitimate basis for data processing, the instruments, such as the GDPR, show that employers who aim to process personal data of workers, may ground the legitimacy of the processing on a wide variety of grounds. Under the GDPR's article 6, processing is considered to be lawful when necessary:

- for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- for compliance with a legal obligation to which the controller is subject
- in order to protect the vital interests of the data subject or of another natural person
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- for the purposes of the legitimate interests pursued by the controller or by a third party.

Hereafter, we discuss the most relevant in more detail. Before doing so, however, it is relevant to point to the fact that some legal systems have more specified the issue of legitimate or lawful processing for employment purposes. Comparative examples learn that collective labour law and industrial relations are referred to as possible relevant legitimate grounds of personal data processing.

Comparative examples learn that collective labour law and industrial relations are referred to as possible relevant legitimate grounds of personal data processing.

The **German** legislator, making use of art. 88 GDPR, and through its Federal Data Protection Act (the "BDSG"), adopted specific rules regarding data processing for employment-related purposes. Employment related processing of personal data has to follow the purposes set out in the BDSG. Besides some special cases, the processing of personal data can be justified on various following grounds, including those arising from industrial relations. It is provided that data processing is allowed when this is necessary the exercise or fulfilment of the rights and obligations of the representation of the interests of the employees resulting from a law or a collective bargaining agreement, a works agreement, or a service agreement, or when data processing is necessary to comply with a works council agreement which conforms with art. 88 GDPR.

Another leading example is **France**, where the national data protection authority ("CNIL") has listed a number of legitimate purposes for data processing in the employment context, [116] that not only include individual employment and HR related data processing justifications, such as Recruitment; Administrative management of personnel; Management of remuneration and completion of related administrative formalities; Provision of professional tools to staff; Organization of work; Keeping of compulsory registers; Internal communication; Performing audits, managing litigation and pre-litigation. The French authority also refers to more general manpower career and collective labour relations, such as career and mobility monitoring; training, management of social assistance and relations with employee representative bodies.

[116] Decision n ° 2019-160 of 21 November 2019 adopting a framework relating to the processing of personal data implemented for the purposes of personnel management (Guideline by CNIL) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041798580/.

In light of this, it should also be pointed out that there will be a strong relation between this particular data protection standard and rights under collective labour law of workers and their representatives. We have to detail out, further below, what further analysis can be made from this relationship, as the legitimacy must be grounded in – and be in conformity with – the GDPR.

b. Legal obligation

The **GDPR** makes data processing legitimate "for compliance with a legal obligation to which the controller is subject".

This is relevant for personal data processed in the employment and HR purposes, as well as for the industrial relations context. The processing of human resources data may be required because of the employer's specific salary or social security obligations arising from employment legislation. The question arises if this ground of processing ('legal obligation') also has potential for legal systems that provide a legal obligation for employers to engage in information and consultation, or collective bargaining activities with workers' representatives. Such obligations, arising from labour law, could thus constitute a possible legitimate ground of personal data processing.

The GDPR's preamble mentions that "*where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament"* as long as such a legal basis is sufficiently "clear and precise" and its application is foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.[117] However, it is rather unclear which types of legal obligations are covered by this legal basis.[118] It is understood "*as relating only to obligations that originate directly from a provision in the law and not from any contractual stipulation between private natural or legal persons*".[119]

The question, however, remains whether the existence of legal obligations to engage in information and consultation, or to engage in collective bargaining, arising from both legislation or collective agreements, will meet the conditions of sufficient 'clarity, precision and foreseeability' as mentioned here above. While the GDPR does not require a specific law for each individual data processing, the question remains which qualitative conditions must be related to the 'legal obligation', as a basis for processing operations. In this respect, article 6, 3(b) of the GDPR provides that the purpose of the processing "shall be determined in that legal basis". This suggests that the relevant (national) law would need to be sufficiently precise in terms of specifying the purposes, and perhaps also other conditions, of data processing resulting from the legal obligation concerned. The GDPR's preamble, further suggests that this law "could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing".[120] However, this rather detailed outlining does not result from the strict obligations of the text of the GDPR provisions themselves.

[117] Recital 41 Preamble GDPR.
[118] Waltraut Kotschy, Article 6. Lawfulness of processing In: The EU General Data Protection Regulation (GDPR). Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press (2020), 332.
[119] Waltraut Kotschy, Article 6. Lawfulness of processing In: The EU General Data Protection Regulation (GDPR). Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press (2020), 332.
[120] Recital 45 Preamble GDPR.

In this regard, the European Working Party, in its opinion WP29, mentions the example of employers who must report salary data of their employees to social security or tax authorities.[121] WP29 identifies several requirements as regard to the notion "legal obligation":[122]

- The obligation must be imposed by law.
- This law must fulfil all relevant conditions to make the obligation valid and binding.
- This law must comply with data protection law, including the requirement of necessity, proportionality and purpose limitation.
- The obligation is imposed by the laws of the European Union or of a Member State.
- The data controller cannot choose whether or not he fulfils the obligation.
- The legal obligation must be sufficiently clear as to the processing of personal data it requires.

These seem to be rather strict conditions and not as such supported by the GDPR text itself. Besides this, it can also be wondered how realistic this condition is in the practical reality of European legal systems. It remains thus a question whether information and consultation rights and obligations under, existing labour laws, will *as such* give sufficient legal basis for personal data processing.

We are of the opinion that information rights in industrial relations law give a legal basis for the disclosure of personal data. In the German works council case, referred to in the previous chapter, it was found that the general right to information contained in a statutory provision can justify the necessity of personal data processing. The fact that such labour laws have in principle a clear logic and purpose would, however, be in favour of a supportive view. It remains open for debate what exactly the GDPR requires where it mentions (in article 6,3,b) that the purposes of processing have to be determined in the relevant legal basis. At least, the GDPR does *not* require that the relevant labour law obligations themselves provide for an explicit mandate or permission to process personal data. Furthermore, these requirements are not mentioned in the case law of the CJEU. The CJEU has recognized in several cases that the compliance with a legal obligation may considered as a ground for legitimation, although the legal provisions did not refer expressly to the safeguards regarding the protection of personal data. The Court considered legal provisions that oblige data controllers to process personal data, such as the obligation to keep a register and to disclose information on "*the appointment, termination of office and particulars of the persons*"[123] or the obligation to keep a record of the working times of workers and to make this information available to the national authority responsible for monitoring working conditions.[124]

We are of the opinion that information rights in industrial relations law give a legal basis for the disclosure of personal data.

[121] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 19.
[122] Ibid, 19-20.
[123] CJEU 9 March 2017, no. C398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vSalvatore Manni, §42.
[124] CJEU 30 May 2013, no. C342/12, Worten – Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT),§45. This case law is also confirmed in CJEU 19 June 2014, no. C683/13, Pharmacontinente – Saúde e Higiene SA,Domingos Sequeira de Almeida, Luis Mesquita Soares Moutinho, Rui Teixeira Soares de Almeida, André de Carvalho e Sousa v Autoridade para as Condições do Trabalho (ACT).

c. Performance of a contract

According to the GDPR, the processing of personal data can also be justified "for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".

This will give a broad justification in the employment context to process workers' personal data, as relationships are in general based on agreements, either employment contracts or other contracts for work or services. According to the EU Working Party's view in Opinion WP29, this legal ground for processing of personal data covers two scenarios. The first scenario is the situation where the data subject is a party of the contract for which the processing of his or her personal data is necessary.[125] The other scenario concerns the processing of data which takes place prior to entering into a contract.[126] A possible example of this scenario is the processing of addresses, names and other personal information of job applicants in context of recruitment.

From the approach of the GDPR, it could also be envisaged that collective agreements play a role in the legitimacy of personal data processing. On the one hand this could be justified on the basis of the 'legal obligation' ground of the GDPR. As the GDPR's preamble mentions that, in order to establish a legal basis, it "*does not necessarily require a legislative act adopted by a parliament"* as long as "such a legal basis responds to the requirements of clarity, precision and foreseeability.[127] This means that there does not seem a reason to exclude – '*a priori*' – information obligations arising from collective labour law as a legitimate ground of processing. Put otherwise, also collective agreements could constitute a legitimate ground of personal data processing. This will probably be the case for agreements that are binding to the parties under national law *and* which have been declared universally applicable,[128] and which are thus sufficiently embedded in the legal system that they meet the conditions of clarity, precision and foreseeability as mentioned here above.

> "Collective agreements (which have been declared universally applicable) could constitute a legitimate ground of personal data processing."

On the other hand, collective agreements could constitute a legal basis to the extent that they can be considered – in light of the GDPR – as a contract, of which the conclusion or performance may require the processing of personal data. However, this would rather justify the processing of personal data of the signatory parties to the (collective) agreement rather than third parties' personal data. The GDPR's provision is rather clear in requiring the only data can be processed related to parties to the contract. It would thus be less evident for workers' representatives to use this basis to justify information of third parties' (workers') personal data.

d. Legitimate interest

The analysis regarding the 'legal obligation' or 'performance of a contract', as a grounds of personal data processing, needs to be set off against the other provisions of the GDPR related to legitimacy of processing, including the rights and interests of others (including third parties), arguably including 'contractual interests' (e.g. the employer). The principles and examples show that the requirement of legitimacy or lawfulness, in light of purposes related to the broad employment context, offers quite open justifications for the processing of personal data, including not only the necessity for the

[125] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 16.
[126] Ibid, 18.
[127] Recital 41 Preamble GDPR
[128] See for this notion, Article 3.8, Posting of Workers Directive 96/71 of 16 December 1996.

employment contract but also "legitimate interests pursued by the controller" (as a rule, the employer). The **German** example shows that the concrete application of the legitimacy principle, laid down in legislative standards, will still rely on case law, from which a broader reasonableness test may result, allowing to see necessary processing also in light of the employers' economic business efficiency or for the application of IT policies.[129] Further below, this relevance is elaborated and examples are given in combining the legitimacy requirement with the proportionality principle, in order to assess which personal data can be seen as 'necessary' and thus can be lawfully processed in the employment context.

Data protection standards thus show that personal data processing is not only legitimate when employers are *required* or *obliged* to process these data, based on legal obligations, but also in case where employers have a contractual or other "legitimate interest".

"Data protection standards thus show that personal data processing is not only legitimate when employers are required or obliged to process these data, based on legal obligations, but also in case where employers have a contractual or other "legitimate interest"."

Justifications may come from the employer's legitimate interests in areas such as: recruitment and selection; the exercise of his rights, such as the right to exercise authority and control, or to direct the enterprise and plan the work, under the employment contract; payroll, administration and human resources services; health and safety obligations and actions; diversity policies, and so on. It would be logical to also imply the employers' rights and interests in collective labour law and industrial relations in this broad sphere of legitimate processing.

Furthermore, also a *public interest* reason could be envisaged by an employer to process personal data related to workers. It means that *external* circumstances to the business, such as for example a pandemic, might determine the necessity to collect some data of workers.

The GDPR gives a set of employment related purposes when referring to employment related data processing in its article 88. It seems evident that the explicit reference means that the European legislator considers these as legitimate purposes:

> "the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship."

The GDPR thus makes explicit that "the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment" are acceptable, legitimate purposes of data processing. It also refers to "obligations laid down by collective agreements".

"It is fair to hold that the GDPR supports obligations and benefits arising from collective agreements as legitimate purposes of data processing".

It is thus fair to hold that the GDPR supports obligations and benefits arising from collective agreements as legitimate purposes of data processing.

[129] German Expert Response.

It should be noted that, when the data processing is based on the legitimate interests of the data controller or third parties, a balancing test has to be carried out. Interests of the data controller have to be balanced against interests or fundamental rights and freedoms of the data subject.[130] The Working Party (WP29) requires that the interests are clear, real and present.[131] Some interests may be beneficial to the society at large (for instance the interest of the press to publish information). But this is not a legal requirement under the GDPR. So also the economic interest of a company,[132] are recognized as legitimate interests, therefore also the common interests of social partners in industrial relations.

> "Economic interests of a company, are recognized as legitimate interests, therefore also the common interests of social partners in industrial relations".

e. Consent

A specific ground of justifying personal data processing is consent from the data subject. It is widely referred to in data protection instruments. However, the 'freedom' of consent is an important issue in data protection law. Consent is obviously only a valid ground if it is, or can be, given freely.

In data protection law, consent is often found problematic in the employment context.

Article 4, 11 GDPR defines consent as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*". The GDPR provides furthermore that, when assessing whether consent is given freely, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[133] Furthermore, the GDPR provides that data subjects have the right to withdraw their consent at any time.[134]

> "Consent is often found problematic in the employment context. Furthermore, the GDPR provides that data subjects have the right to withdraw their consent at any time."

The European Working Party has delivered its views on this point and shares the idea of the problematic nature of consent in employment relationships. It is of the opinion that, "unless in exceptional situations, employers will have to rely on another legal ground than consent – such as the necessity to process the data for their legitimate interest".[135] It furthermore states that default settings on devices or the application of software cannot qualify as consent given from employees, as consent would require an "active expression of will".[136]

The GDPR gives some instruction about the *form* of consent. It can be assumed that, ideally, the data subject's consent is given in the context of a written declaration. But other methods may be applicable, including electronic methods. Preamble 32 of the GDPR clarifies, however, that silence, pre-ticked boxes or inactivity do not constitute consent. Indeed, consent should be given by a clear affirmative

[130] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 23.
[131] Ibid.
[132] Ibid.
[133] Article 7, 4 GDPR.
[134] Article 7, 3 GDPR.
[135] WP Opinion 2/2017, 4.
[136] WP Opinion 2/2017, 7.

act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her.

Whether individual worker consent would be a legitimate ground of personal data processing in light of collective bargaining or worker representation functions of representatives and trade unions, remains rather unclear. It could be argued that this may be in the own advantage of the workers themselves who are concerned in negotiations or in consultations. Nevertheless, the legal environment is still rather uncertain for relying on individual consent of workers in this context.

d. Sensitive data

Attention has to be paid when special categories of personal data (health data[137], information on trade union membership[138],…) are processed. Data concerning health are defined in the GDPR as "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*".[139] This notion is interpreted rather broadly. This is shown in the German benchmark case, reported above, in which the court considered data related to the maternity leave and, therefore, the pregnancy of employees as health related data. Hence, in the context of industrial relations it may occur that these 'special data' are processed when information is exchanged between employers, workers' representatives and trade unions.

The paragraph below shows the importance to examine whether or not special categories are exchanged in the particular data flows.

The GDPR prohibits the processing of these special categories of personal data, unless an exception applies. The GDPR provides following exceptions especially relevant in the context of industrial relations in which the prohibition does not apply:

- The data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes. WP29 mentions that if no other exception applies the employer can rely on the explicit consent of the worker concerned.[140]
- The processing is necessary for the purposes of **carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment**. According to WP29, this exception can have a wide effect and it will depend of national legislation which obligations and rights of employers are set out in employment law.[141]
- The processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a foundation, **association** or any other not-for-profit body with a political, philosophical, religious or **trade union aim**. The GDPR refers to the 'specific needs' of legitimate activities by associations which have the purpose to exercise the fundamental freedoms.[142] By referring to the specific needs, this exception may have a rather restrictive

[137] WP29 mentions in this regard following examples information in connection with pay during sickness, meeting health and safety requirements, providing an occupational health scheme, providing insurance or pension benefits. WP29, Opinion 8/2001 on the processing of personal data in the employment context, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf, 17.
[138] WP29 mentions in this regard the example of enabling the employer to deduct trade union subscriptions from salary on behalf of the trade union. WP29, Opinion 8/2001 on the processing of personal data in the employment context, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf, 17.
[139] Art. 4. 15 GDPR
[140] WP29, Opinion 8/2001 on the processing of personal data in the employment context, 16.
[141] WP29, Opinion 8/2001 on the processing of personal data in the employment context, 17.
[142] Recital 51 GDPR

scope. This would mean for trade unions' activities that only data related to the membership of trade unions may be processed.

Most importantly, the GDPR does not allow processing of special categories of personal data on the basis of *legitimate interests* of data controllers or third parties. Disclosure of personal data in light of industrial relations would thus need to be justified on the basis of legal obligations arising from industrial relations laws (related to information and consultation). The explicit consent of the data subject, as a way out, is for various reasons (see above) less evident.

3.3. Proportionality

There are different ways to label and define a set of principles related to personal data protection that are related. Conditions of relevancy, adequacy, necessity, or proportionality of data processing are all related to the additional requirements and limitations of data processing, beyond the above mentioned condition of lawfulness or legitimacy.

Proportionality would seem the most general and over-arching term encompassing those principles. It allows to understand the term 'necessary' and to distinguish it from 'legitimacy', since the legitimacy principle is also referring to as necessity, such as in "necessary for the performance of a contract" (cf. (art.6,1,b) **GDPR**. While the lawfulness or legitimacy criteria refer to grounds, reasons or purposes of data processing, the requirements of relevance, adequacy and so on, would rather point at the relationship of the personal data that are collected and processed, with those purposes. As necessity should be evaluated in light of the aim pursued,[143] the processing has to remain proportionate to the legitimate purposes.[144] In the words of the European Working Party: "Regardless of the legal basis for such processing, a proportionality test should be undertaken prior to its commencement to consider whether the processing is necessary to achieve a legitimate purpose".[145]

The proportionality principle is explicitly mentioned as a principle in most major documents on data protection, such as **CoE Convention 108**. In some instruments, proportionality is seen to be included in the principle of "data quality", such as in the **OECD Guidelines** (2013). But all instruments use one or more of the principles of relevance, adequacy, non-excessiveness, and so on. The **CoE Recommendation** (2015), relating to employment, provides, for example (in section 5.2.) that personal data collected by employers for employment purposes should be "relevant and not excessive, bearing in mind the type of the employment as well as the changing information needs of the employer". What must be clear is that the proportionality limits the use of personal data. It, however, does not *a priori* exclude any processing of personal data. It rather guides data processing to a quality and balancing process. In light of this, it should be noted that the principle of proportionality is inherent to human rights protection mechanisms, as limitations to human rights should not only respond to a legitimate aim, but also be proportionate. While different approaches of proportionality could be envisaged, three main explanations are broadly accepted as constituting a test of proportionality in the context of data protection law:[146]

> "The proportionality principle limits the use of personal data. It does not a priori exclude any processing of personal data."

[143] Section 4.1 CoE Rec 2015.
[144] WP Opinion 2/2017, 7.
[145] WP Opinion 2/2017, 4.
[146] Lee A. Bygrave, "Core principles of data privacy law", in *Data privacy law. An international perspective*, OUP, 2014, p.148.

- Suitability (or adequacy): is the data processing suitable or relevant to realising the legitimate goals?
- Necessity: is the data processing required for realizing the legitimate goals? Such necessity requirement may be connected to an alternative means test: are there alternative means to realise the legitimate goals.
- Non-excessiveness: does the measure go further than is necessary to realise the legitimate goals?

A new language, developed in the GDPR, is 'data minimization'. According to article 5, 1, c **GDPR**, the processing of personal data should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')". Also the **CoE Recommendation** (2015) provides (section 4.1.) that "employers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned".

Data protection instruments usually do not offer a straightforward answer to the question of whether and, if so, to what extent, employers may thus process personal data in the workplace context. Both the open grounds of lawfulness and legitimate purposes of data processing (under the 'legitimacy principle') and the proportionality or necessity test in light of these purposes, do not take away that a wide series of personal data can be processed in the context of employment. Different examples show the number and kind of data that employers are allowed to process, taking into account legitimate purposes. The European Working Party, in its **Opinion 8/2001** mentioned the following data as possible relevant data in the employment context:[147]

- Application forms and work references-
- Payroll and tax information-tax and social benefits information
- Sickness records
- Annual leave records
- Unpaid leave/special leave records
- Annual appraisal/assessment records
- Records relating to promoting, transfer
- Training, disciplinary matters
- Records relating to accident at work
- Information generated by computer systems
- Attendance records
- Family members
- Reimbursement of expenses, e.g. travel

The need to collect and further process personal data in the employment relationship, and the establishing of all kinds of employee records, is confirmed in different jurisdictions.

[147] Working Pary, Opinion 08/2001 on the processing of personal data in the employment context, WP 48, 13 September 2001, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/

files/2001/wp48_en.pdf

3.4. Purpose limitation

a. Principle

The purpose limitation principle is a key principle of personal data protection standards. The processing of personal data for purposes *other* than those for which the personal data were *originally* collected, should be allowed if the processing is *compatible* with the original collection purpose.

It means that 're-purposing' is, in principle possible, but this should be compatible with the original purpose of collection.

The purpose limitation principle is a widely recognised principle of data protection. This general requirement comes back in most data protection instruments. The different international data protection standards share the rule that personal data should be processed for specific (or specified), explicit, legitimate (or lawful) purposes. Furthermore, personal data should not be further processed in a manner incompatible with those purposes. This important data protection principle is related to verifiability and transparency of personal data processing. It also contributes to the fairness of data processing.

> "Processing of personal data for purposes *other* than those for which the personal data were *originally* collected, should be allowed if the processing is *compatible* with the original collection purpose."
>
> "This may concern the *secondary* use of personal data of workers in an industrial relations context."

The purpose limitation principle is of course relevant and interesting in light of the scope this study, as this may concern the *secondary* use of personal data of workers in an industrial relations context that were originally collected by employers in the context of human resources or personnel administration.

b. Compatibility assessment for secondary use

In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia:

> all relevant circumstances of the case, including key factors:
>
> - relationship between the original purposes and the (new) purposes of further processing;
>
> - the context in which personal data have been collected and the reasonable expectations of the data subjects as to their further use;
>
> - the nature of the personal data and
>
> - the impact or consequences of the further processing on the data subjects;
>
> - safeguards adopted to ensure fair processing.[148]

The purpose limitation principle, while thus being open for 'change of purpose' (within the confines of compatibility) is surrounded with additional data protection standards that give more detailed obligations. The **ILO Code of Practice** provides:

> 5.3. If personal data are to be processed for purposes other than those for which they were collected, the employer should ensure that they are not used in a manner incompatible with the original purpose, and should take the necessary measures to avoid any misinterpretations caused by a change of context.

[148] Cf. Article 6.4 GDPR; Working Party Opinion 03/2013 on purpose limitation, p. 40.

Part of the respect of secondary (re-purposed) use of personal data of workers can be the respect for transparency and information to the worker concerned. For example, the **CoE Recommendation** (2015) provides:

> 6.3. Under exceptional circumstances, where data are to be processed for employment purposes other than the purpose for which they were originally collected, employers should take adequate measures to avoid misuse of the data for this different purpose and inform the employee. Where important decisions affecting the employee are to be taken, based on the processing of that data, the employee should be informed accordingly.

It is also clear that the secondary use of personal data is relevant in light of corporate restructuring. When there is, for example, a transfer of undertaking and companies are merged or otherwise transferred, the question is what happens not only with the workers, but also with the personal data of those workers. For example, the **CoE Recommendation** (2015) points at this issue:

> 6.4. In the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principles of proportionality and purpose specification in the subsequent use of data. Every substantive change in the processing should be communicated to the persons concerned.

c. Compatibility levels

According to the EU Working Party, different levels can be distinguished in the legal assessment of compatibility of data processing (including data sharing) with the original purposes of collecting personal data. In practice different scenarios may play a role in this assessment.

- *Scenario 1: Compatibility is prima facie obvious:* In many cases, further processing of personal data may be found compatible, as "the processing clearly meets the reasonable expectations of the data subjects", even if not all details were fully expressed at the start.

- *Scenario 2: Compatibility is not obvious but still justified:* In this situation, there is a 'connection' between the specified purpose and the way the data are subsequently processed. Either the purposes "are related but not fully matching", or data are further used "for different and not directly related" purposes, but their relationship or the context would still justified the secondary use. In this case, additional safeguards may be put in place in order to "compensate for the change of purpose (e.g. to provide additional information and explicit options for the data subject)".

- *Scenario 3: Incompatibility is obvious:* It concerns the further use of data for additional purposes that a reasonable person would find "not only unexpected, but also obviously inappropriate or otherwise objectionable".

In order to have an 'obvious incompatible purpose' of further use or processing of personal data, it should concern a rather clear case.

Clearly incompatible purposes refer to cases where it is beyond doubt that the new purposes would amount to unfair processing.

In HR-related data protection discussions, examples mostly relate to personal data that are later used to the detriment of workers.

"Clearly incompatible purposes refer to cases where it is beyond doubt that the new purposes would amount to unfair processing."

Example 1:

In this context, the **ILO Code of Practice** provides, in section 5.4, that "personal data collected in connection with technical or organizational measures to ensure the security and proper

operation of automated information systems should not be used to control the behaviour of workers."

Example 2:

Another example of incompatible secondary use, appeared before the European Civil Service Tribunal. In the case of "V",[149] a candidate was refused by the European Commission after being held unfit for hiring by the European Commission's Medical Service. When she was, later on, offered a post with the European Parliament, a copy of her medical file from the Commission's medical service was transferred to the Parliament. According to the Tribunal, it concerned sensitive data which could not just be transferred to another institution without the individual's consent. Using the same data to determine her fitness for the post with another EU institution was seen as an incompatible a 'change of purpose'.

The latter case also makes clear that the sharing of information with a third party, even when the same purposes apply as during the time of collection, may lead to a 'change of purpose'. Also here, the degree of fairness and the detrimental impact on data subjects is likely to play a role in the assessment.

"The sharing of information with a third party may lead to a 'change of purpose'."

Example 3:

In the industrial relations context, and as described in the problem cases in the introductory examples in this study, the issue may arise as to whether workers' representatives have access to the ICT system of employers and whether, for example, trade union delegates would have access to the e-mail addresses of staff members. While the issue of legitimacy may most likely be overcome, the purpose limitation principle – and the compatibility question – may stand in the way.

This third example, in our view, would be a case where "compatibility is not obvious but still justified".

A relevant European institution's staff case concerns the use of the internal e-mail system for trade union activities. A trade union member and staff member working for the European Central Bank, was informed by the management to have *abused* the e-mail system of the ECB. She was warned that the sending of e-mail messages addressed to all ECB staff required management authorization and that this cannot be circumvented because of trade union reasons. The management stored its communication with the staff member about this affair in her personal file. The Court found that the inclusion of this communication in the personal file of the staff member constitutes processing of personal data, but it also found that the ECB may be entitled to consider that inclusion is necessary for the performance of the employment contract. It may be relevant according to the Court for the assessment of the staff member's conduct in the service.[150]

[149] *V & EDPS v. European Parliament*, 5.7.2011, F-46/09.
[150] T-320/02, *Esch-Leonhardt and Others v. European Central Bank*, 18.2.2004.

The issue shows how GDPR and labour law obligations can be linked. For example, the ILO Workers' Representative Recommendation n° 143 of 1971 provides that the management should make available to workers' representatives, *material facilities and information as may be necessary for the exercise of their functions*. This issue could be interpreted as also covering access to electronic communication tools.[151] Although this right would still need to be made more robust, the ILO Committee on Freedom of Association held that "workers representatives should enjoy such facilities as may be necessary for the proper exercise of their functions, including the use of email." It also stated that, "although the modalities for the use of email in the workplace by trade unions should be a matter for negotiation between the parties, in the event that the union organization is able to use its own email account from the workplace to contact its members, the fact that trade union communications must be sent using the institutional email address of the organization, and not the firms email address, does not appear to limit the principles of freedom of association."[152]

The ILO's supervisory body's view is that access to electronic communication tools should be guaranteed under international labour law. To the extent that a legitimate ground can be indicated, the purpose compatibility for the use of the communication tools (e.g. including e-mail addresses) could be strengthened.

It would thus be dependent on circumstances, although the ILO's supervisory body's view is that access to electronic communication tools should be guaranteed under international labour law. To the extent that a legitimate ground can be indicated, the purpose compatibility for the use of the communication tools (e.g. including e-mail addresses) could be strengthened.

From the limited guidance, the consideration of alternatives and proportionality will clearly play a role. This will also include a data minimization strategy. As indicated above, in this case, additional safeguards may need to be put in place in order to "compensate for the change of purpose (e.g. to provide additional information and explicit options for the data subject)".

The consideration of alternatives and proportionality will play a role. Additional safeguards may need to be put in place.

d. Additional safeguards

Some additional safeguards will positively influence the assessment of compatibility in case of further processing of personal data for new purposes. A change of purpose can be compensated by appropriate additional measures.[153] Some of theses safeguards may be:

- **Anonymisation/Pseudonymization**

According to the EU Working Party, "*full or partial anonymisation, in particular, can be relevant to the safe use or sharing of data within organisations, particularly large ones with diverse functions*".[154]

- **Transparency**

[151] F. Dorssemont, Facilities for trade union officials and members to exercise their rights – a comparative review, July 2020, https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_760829.pdf.

[152] Compilation of Decisions of the Committee on Freedom of Association, ILO, nrs. 1600-1601, https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:70002:0::NO::P70002_HIER_ELEMENT_ID,P70002_HIER_LEVEL:3949093,1.

[153] Working Party, Opinion 2/2017 on data processing at work, 26.

[154] Working Party, Opinion 2/2017 on data processing at work, 26.

Secondary use of personal data, collected for HR purposes, may also become more legitimate when transparency is provided to data subjects. The secondary use of personal data is, for example, also relevant in light of corporate restructuring. When there is, for example, a transfer of undertaking and companies are merged or otherwise transferred, the question is what happens not only with the workers, but also with the personal data of those workers. In light of this question, the **CoE Recommendation** (2015) points at this issue that "every substantive change in the processing should be communicated to the persons concerned".

It would seem to suggest that data processing is not becoming impossible when more parties are involved in the personal data, but there should be some transparency when there is a substantive change in the processing.

- **Informational control (opt-out/consent)**

In case of further use of processing with change of purpose, a relevant aspect may be the degree of control given to the data subjects concerned. An opt-out system could be envisaged, implying that data subjects are informed about change of purpose and are able to react to it by requiring that their names or data relating to them are withdrawn from the processing. In some cases, requesting a specific separate consent for the new processing may help to compensate for the change of purpose.[155]

- **Positive context** :

Creating or maintaining a positive context may support a modified purpose. For example, it would not be recommended to process data for a secondary purpose with a potential negative impact on the data subjects (workers) concerned (for example, possible disciplinary action).

e. Purpose specification

It is obvious that *compatibility* discussions can be avoided by including industrial relations objectives in the *original* purposes of data collection/data processing. This would mean that HR related data, when collected by employers, also include industrial relations as one of the purposes for which the data can/will be used. This will be an action to be undertaken by the employer.

In this context, it needs to be pointed out that data processing purposes must be sufficiently clear. According to the EU Working Party, "the purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied."[156]

According to the European Working Party, "a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'."[157]

It will be thus advisable to indicate a purpose description which is more precise, such as, that data are/may be processed:

[155] Working Party Opinion 03/2013 on purpose limitation, p.26-27.
[156] Working Party Opinion 03/2013 on purpose limitation, p15.
[157] Working Party Opinion 03/2013 on purpose limitation, p16.

- 'to inform [listed] workers' representatives at company level, or within a group of undertakings to which the company belongs, with a view to respect the applicable laws on information and consultation and/or to consultation with the representatives'.
- 'to inform [listed] trade union representatives at company or sectoral level, or within a group of undertakings to which the company belongs, with a view to make an agreement on working conditions'.

This is an action that will be undertaken by the employer as the prime collector and processor of personal data.

3.5. Access to personal data

All major data protection instruments provide that every data subject has the right of access to personal data (concerning him or her) as well as the right to have the data rectified. Under these principles, a set of additional data protection rights for data subjects are provided in nearly all frameworks:

- **Access**: the right to obtain access to personal data is universally acknowledged.
- **Rectification**: is often a follow up right of the right to access and recognized in all data protection instruments.
- **Deletion/erasure**: is strongly connected to access and rectification and is also a universally accepted right
- **Data portability**: less globally recognized, but it appears in the GDPR.

The right to have access to personal data will inevitably play a role in the employment context, seen the number of data and records kept for reasons of personnel administration, or more generally human resources, and possibly other purposes. Workers may demand access to personal data relating to them from employers that are holders, and thus controllers, of these data.

The right to access may also play a role in the *IR* context. According to the ILO, workers should be entitled to designate a workers' representative to assist them in the exercise of their right of access.

In light of this, the right to access – and rectification – may also play a role in the *IR* context. According to the **ILO Code of Practice**,[158] workers should be entitled to designate a workers' representative or a coworker of their choice to assist them in the exercise of their right of access.

a. Access

According to the GDPR "modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data".[159] The right to have access to personal data processing may, additionally, involve a right to receive a copy of the personal data undergoing processing.[160]

[158] Section 11.5 ILO Code of Practice.
[159] GDPR, Recital 59.
[160] Cf. article 15, 3 GDPR.

b. Rectification

Data subjects have generally the right to obtain the rectification of inaccurate personal data concerning them. This also has a logical relevance for the employment context. However, some discussions may arise, certainly with regard to whether data are complete or whether evaluation data can be rectified.

Whether personal data should be rectified, or completed, may be subject to interpretation and discussion. In light of this, it is accepted that a worker is entitled to put a statement in the relevant record, with an indication of the worker's disagreement with the personal data. This finds support in article 16 of the GDPR, which guarantees "the right to have incomplete personal data completed, including by means of providing a supplementary statement".

c. Evaluation data

A point of discussion relates to evaluation data. One may understand the issue in terms of worker evaluations made by employers or supervisors, or test results, which are often kept in personnel files.

Generally, there is few guidance on the issue. International data protection standards do not seem to give a direct answer on how to treat evaluation data, while different *national* laws do qualify opinions as personal data.[161] It would seem obvious that a person's own opinion concerns personal data relating to that data subject. The question is, however, whether a person's opinion concerning another individual, such as the evaluation of a worker by a supervisor, can be seen as personal data, and whose personal data.

The **ILO Code of Practice** is rather clear and straightforward and refers to "judgmental" data under its personal data protection principles for workers:

> 11.12. In the case of judgmental personal data, if deletion or rectification is not possible, workers should have the right to supplement the stored personal data by a statement expressing their own view. The statement should be included in all communications of the personal data, unless the worker agrees that this is not necessary.

The **CoE Recommendation** (2015) provides:

> 11.3. The right of access should also be guaranteed in respect of evaluation data, including where such data relate to assessments of the performance, productivity or capability of the employee when the assessment process has been completed at the latest, without prejudice to the right of defense of employers or third parties involved. Although such data cannot be corrected by the employee, purely subjective assessments should be open to challenge in accordance with domestic law.

The **European Court of Justice** (CJEU), in a judgment of 20 December 2017, dealt with the case of *Nowak v. Data Protection Commissioner*[162]. In its judgement, the CJEU is of the opinion that the comments of an examiner with respect to a candidate's answers, no less than the answers submitted by the candidate at the examination, constitute information relating to that candidate. According to the Court, the content of those comments reflects the opinion or the assessment of the examiner of the individual performance of the candidate in the examination, particularly of his or her knowledge and competences in the field concerned. The purpose of those comments is, moreover, precisely to record the evaluation by the examiner of the candidate's performance, and those comments are liable to have effects for the candidate. Therefore, the data subject has a right of access to the data relating to him. The Court recognises that this does not imply a right to change the exam answers afterwards, but the right to access enables the data subject to obtain, depending on the circumstances,

[161] Cf. Lee A. Bygrave, *Data privacy law. An international perspective*, OUP, 2014, p134.
[162] CJEU, Judgment of 20 December 2017, No. C-434/16, *Nowak v Data Protection Commissioner*, ECLI:EU:C:2017:994.

rectification (e.g. material mistakes by the examination authority), erasure or blocking of the data (e.g. when communication to third parties is intended).

With regard to worker evaluation reports, workers will thus, in our view, be able to exercise a right to access to evaluations made about them. A nuance is, however, important. Evaluation reports are not completely the same as examinations or tests, although there seems to be no reason to exclude also these data from the protection offered by data protection legislation in the way the European case has been dealing with it. A possible limitation might be that, in an HR context, evaluations may imply information of other workers (colleagues) who have a right and interest of not having their information disclosed in light of the exercise of data protection rights of another employee. But the employer would nevertheless need to make reasonable steps to still inform the data subject, for example in the form of a summary.

With regard to worker evaluation reports, workers will thus, in our view, be able to exercise a right to access to evaluations made about them.

d. Erasure

The right to erasure implies the right to have data removed. This could mean different things in an employment context. It could imply that some data have to be partly removed, so that another and more proper picture is given of the available information. Under certain conditions, the GDPR also provides for a right to erasure, or a 'right to be forgotten' for the data subject, meaning the right to obtain from the controller the erasure of personal data.[163] According to the GDPR's Preamble (paragraph 65) a data subject should have a right to be forgotten "*where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed*".

e. Data portability

Data portability has become relevant with the rise of the network economy, where not only networks of enterprises, people and services are strongly interconnected, but also where "information rules".[164] In this context, a degree of control or self-determination with regard to information, as well as a form of ownership of the data subject, is recognised. Data portability refers to the right to receive personal data form a data controller and/or to transfer those data to another controller.

Notwithstanding its growing relevance, the principle of data portability has not yet been expressed in specific terms in many international data protection standards. Only the **Ibero-American Standards** and the **GDPR** appear to explicitly include it. However, the approach of the **Declaration of Principles of Freedom of Expression and Access to Information in Africa (2019)** is also interesting in this respect, stressing the informational autonomy of data subjects:

> Principle 42. 4. Every person shall have the right to exercise autonomy in relation to their personal information by law and to obtain and reuse their personal information, across multiple services, by moving, copying or transferring it.

The GDPR (article 20(1)) states that:

> "*The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable*

[163] Article 17, 1 GDPR.

[164] Carl Shapiro & Hal R. Varian, *Information Rules: A Strategic Guide to The Network Economy*, Harvard Business Review Press, 1998, 352p.

format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided".

The right to portability is at least granted by the GDPR apply where the data subject provided the personal data on the basis of his or her consent or a processing which was necessary for the performance of a contract.

Data portability may for example be relevant in cases of evaluation data, which could be relevant for new employment positions that workers take up with other employers. It may also be relevant specifically in the context of the gig economy and platform work, where workers have an interest in moving rating and ranking systems from one platform to another.[165]

Data portability also may be situated within the 'gig worker' field, where platforms share information with other service providers and/or consumers.

3.6. Key findings

- ✓ Three main and essential data protection principles are: Legitimacy; Proportionality; Purpose Limitation.
- ✓ The principles also apply to disclosure of data to workers' representatives and trade union members.

Legitimacy:

- ✓ The (employment) contract will be a strong basis for the HR data collection by employers
- ✓ On disclosure of personal data in an industrial relations context, there is – overall – less existing guidance.
- ✓ We are of the opinion that information rights in industrial relations law give a legal basis for the disclosure of personal data.
- ✓ Personal data processing is not only legitimate when employers are required or obliged to process these data, based on legal obligations, but also in case where there is a contractual or other "legitimate interest".
- ✓ Consent is not an evident legal basis: it is often found problematic; should be organised on specific conditions; data subjects have the right to withdraw their consent at any time.

Proportionality:

- ✓ Data processing (including disclosure) should always be balanced with the rights of data subjects.
- ✓ Showing the *necessity* to process personal data will be a crucial argument. This necessity may be derived from the need to be able to *effectively* exercise the right to information

Purpose limitation:

- ✓ Processing of personal data for purposes *other* than those for which the personal data were *originally* collected, is only allowed if this is *compatible* with the original collection purpose.
- ✓ Industrial relations may be seen as a compatible *secondary* use of personal data.

[165] Uni Global Union, Top 10 Principles for Workers' Data Privacy and Protection, (cf. point 1.c.), http://www.thefutureworldofwork.org/media/35421/uni_workers_data_protection.pdf?utm_campaign=revue_fortnightly_newsletter&utm.

- ✓ We are of the opinion that HR related data are collected by employers can later be used and shared with workers' representatives.
- ✓ However, there will still be limits resulting from the GDPR, and some secondary (or tertiary) use may be problematic.
- ✓ Specific guarantees may help, such as anonymization, pseudonymization, transparency, opt-out options, creating a positive context for workers.
- ✓ Compatibility problems may be avoided if employers are willing to include data disclosure with workers' representatives in the original purposes of worker data collection

Chapter 4. Governance and tools for GDPR compliance

This chapter focuses on making information and data exchange in industrial relations scenarios compliant with the GDPR. It gives a governance framework and contains toolbox questions for guiding data flows in industrial relations. A data flow chart will be set up and toolbox questions will lead to various conditions, set under data protection law, to strengthen compliance and make data flows possible.

4.1. Introduction

The GDPR provides that data controllers must be held responsible and demonstrate compliance for living up to standards on lawfulness of data protection (cf. art. 5.2 GDPR). The accountability principle is also brought forward in the **OECD Guidelines** (2013), section 14: "*A data controller should be accountable for complying with measures which give effect to the principles stated above*."

Accountability should not be understood in a too narrow sense. The idea is that data controllers must give effect to data protection laws and principles and provide for appropriate safeguards based on privacy risk assessment, ongoing monitoring and periodic assessment. This is why a broader notion of data protection 'governance' is more useful. This also refers to the tools and mechanisms that are available to manage due diligence with regard to personal data protection.

> "Governance refers to the tools and mechanisms that are available to manage due diligence with regard to personal data protection."

Data controllers and other involved parties thus bear a wider responsibility which requires them to be accountable, to provide for sufficient security measures related to data processing activities, as well as to manage and regularly assess data processing activities.

> "The GDPR refers to various tools and mechanisms. It will be a matter of taking an approach which is adapted to the context and situation of the involved data processing and the involved actors."

The whole governance dimension is a highly relevant matter in finding solutions for personal data protection problems and issues. The GDPR refers to various tools and mechanisms to secure that personal data processing is in conformity with the standards. In many instances, reference is made to a case-by-case approach. It will be a matter of taking an approach which is adapted to the context and situation of the involved data processing and the involved actors.

The following relevant issues have to be dealt with:

- Determining and identifying the responsible actors within a GDPR context
- Making a data protection impact assessment
- Selecting appropriate tools and solutions (identifying a governance toolkit)

4.2. Installing a GDPR compliance culture

Privacy by design and by default

The GDPR uses the concepts of 'privacy by design' and 'by default' in relation to accountability applied by the GDPR.

Article 25 GDPR provides:

> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
>
> 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

This means that data controllers have to be proactive and making continuous assessment of the privacy impact of what they decide (and try to limit the privacy impact).[166]

Preamble 78 of the GDPR explains that it entails that appropriate technical and organisational measures are taken to ensure that the requirements of the GDPR are met: "*the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations*."[167]

Shadowing DPIA

A "data protection impact assessment" (DPIA) has been promoted as an important component of personal data protection. Article 35(1) of the GDPR provides that:

> "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks*."

A DPIA is, as a rule, obliged for data processing with a 'high risk' impact or "likely to result in a high risk to the rights and freedoms of natural persons". Which data processing will be of such as high risk, and which not, may be a matter of interpretation. The European data protection authorities have issued some guidelines on this point. However, they have also added that, in cases where it is not clear whether a DPIA is required, it is recommended "that a DPIA is carried out nonetheless, as a DPIA is a useful tool to help controllers comply with data protection law".[168] A 'DPIA' may be relevant in the

[166] L. JASMONTAITE, I. KAMARA, G. ZANFIR-FORTUNA and S. LEUCCI, *Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, 182 EDPL (2/2018).
[167] Preamble 78 GDPR.
[168] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017, p.8.

context of the employment relationship, for example in cases where employers are intending extensive monitoring of workers.[169] An example of 'high risk', according to the European Working Party's **Opinion 2/2017** is "a case of systematic and extensive evaluation of personal aspects related to natural persons based on automated processing".[170] While the processing of personal data within the context of industrial relations may – almost per definition – have an impact on both collective as well as individual positions of workers, the information flows arise from, or in light of, legal obligations in the field of labour law.

In this context, there are **two ways of looking at the DPIA** as mentioned in the GDPR:

- Either it is seen an obligation to be followed in furtherance of article 35 GDPR;
- Or it is seen as due diligence and good conduct and as a way to create a culture of trust and compliance related to personal data protection.

The European Working Party has proposed elements of a DPIA that is in conformity with the GDPR.[171]

- a systematic description of the processing is provided (Article 35(7)(a)):
    - nature, scope, context and purposes of the processing are taken into account (recital 90);
    - personal data, recipients and period for which the personal data will be stored are recorded;
    - a functional description of the processing operation is provided;
    - the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
    - compliance with approved codes of conduct is taken into account (Article 35(8));
- necessity and proportionality are assessed (Article 35(7)(b)):
    - measures envisaged to comply with the GDPR are determined (Article 35(7)(d) and recital 90), taking into account:
        - measures contributing to the proportionality and the necessity of the processing on the basis of:
            - specified, explicit and legitimate purpose(s) (Article 5(1)(b)); o lawfulness of processing (Article 6);
            - adequate, relevant and limited to what is necessary data (Article 5(1)(c));
            - limited storage duration (Article 5(1)(e));
        - measures contributing to the rights of the data subjects:
            - information provided to the data subject (Articles 12, 13 and 14);
            - right of access and to data portability (Articles 15 and 20);
            - right to rectification and to erasure (Articles 16, 17 and 19);
            - right to object and to restriction of processing (Article 18, 19 and 21);
            - relationships with processors (Article 28);
            - safeguards surrounding international transfer(s) (Chapter V);
            - prior consultation (Article 36).
    - risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):

[169] William RM Long, Francesca Blythe, Alan Charles Raul, "EU Overview", in Alan Charles Raul (ed.), *Privacy, Data Protection and Cybersecurity Law Review*, Seventh Edition, Law Research Business Ltd., 2020, p9.
[170] Working Party, Opinion 2/2017 on data processing at work, p8.
[171] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017, p.22.

- origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - risks sources are taken into account (recital 90);
    - potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
    - threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - likelihood and severity are estimated (recital 90);
    - measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- interested parties are involved:
    - the advice of the DPO is sought (Article 35(2));
    - the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).

4.3. Toolbox-questions

Overall, in light of the GDPR, the key-question will be to what extent personal data have to be communicated in order to be able to exercising a right or interest with regard to information as a trade union or a workers' representative, and what is the legal basis. Obviously, a number of related data protection impact questions will also be relevant.

"The key-question will be to what extent personal data have to be communicated in order to be able to exercising a right or interest with regard to information as a trade union or a workers' representative, and what is the legal basis."

In order to make the set of DPIA issues, raised above, sufficiently practical for the industrial relations context of this study, we have narrowed them down to the following key questions.

These questions should, in our view, be addressed when workers' representatives (or trade unions) and employers face an issue of personal data in light of information disclosure in an industrial relations context.

1. What (personal) data flows can be identified ?
2. Who is identified as controller/processor/recipient ?
3. What is the legal/legitimate ground of personal data processing ?
4. Which (personal) data are processed for which purposes?
5. How is personal data processing minimized to what is necessary and proportionate?
6. Have data subjects been informed ?
7. What is the territorial scope of the personal data processing?
8. Are risks to the rights and freedoms of data subjects properly addressed ?
9. Are additional guarantees applicable ?
10. Have interested parties been involved ?

Q1: Which (personal) data flows can be identified ?

a. Analysis

A key aspect is the identification of (personal) data flows. In principle, establishing the data protection impact of each data processing activity would require a case-by-case approach. This is also suggested by the European data protection authorities. At the same time, in order to practically operationalize the field of industrial relations, we propose to distinguish some cases and scenarios on the basis of which the analysis can be made.

This allows for a proper identification of (potential) data flows for which GDPR conditions will need to be applied. In light of this, we provide:

- a set of **model-scenarios** related to information exchange;
- a number of **key-levels** of information exchange;
- a **data flow chart** representing potential data flows between different industrial relations actors.

b. IR models

Industrial relations in Europe and the rest of the world make an interesting but complex phenomenon. A **wide diversity** of rules and practices of representation exists leading to forms of workers' representations in legal and industrial relations systems.

In order to make a sufficiently practical, while taking into account potential diversity, we point at ILO Convention n° 135, which defines the notion of workers' representatives as :

> persons who are recognised as such under national law or practice, whether they are (a) trade union representatives, namely, representatives designated or elected by trade unions or by members of such unions; or (b) elected representatives, namely, representatives who are freely elected by the workers of the undertaking in accordance with provisions of national laws or regulations or of collective agreements and whose functions do not include activities which are recognised as the exclusive prerogative of trade unions in the country concerned.

Therefore, on the one hand, we distinguish systems where representation goes through workplace representation bodies, such as works councils or employee representatives, and on the other hand representation through unions and/or union delegates.

"We distinguish systems where representation goes through workplace representation bodies, such as works councils or employee representatives, and on the other hand representation through unions and/or union delegates".

It is obvious that these distinctions are more than a theoretical perspective, but can often only partly describe complex realities. Workplace representation bodies, with or without union control, do not exclude the presence and a significant role of trade unions, either at company or at sector level. Often, trade unions play a dominant role in workplace representation bodies. In addition, as pointed out in ILO Recommendation 143, in the same undertaking there may be both a trade union representatives as well as an elected workplace representative body.

Nevertheless, taking this into account, a brief classification, as given here, here may also shed light and clarify the responsibilities under the GDPR provisions.

c. Model scenarios

In the introduction of this study, a number of different cases and problem settings have been set out related to the issues of information and data protection. *In globo*, taking into account different frameworks of industrial relations, the cases can be modelled, into **5 typical industrial relations**

scenarios. In order to make the GDPR analysis sufficiently employable in the broader IR field, but also to sufficiently highlight their characteristics in terms of their data protection impact, it is relevant to distinguish them in a sufficiently abstract manner.

The proposed model scenarios are:

1. **Collective representation**: this is the case where workers' representatives exercise their normal rights of information and consultation in the context of workplace representative settings, either trade union or non-trade union driven, according to national (and/or European) legislation or agreements relating to information and consultation rights in the company.
2. **Implementation**: this is the case where workers' representatives wish to verify, on the basis of information, whether employers live up to collectively set or agreed working conditions. This, for example, covers the case of monitoring whether agreements or systems related to seniority are properly applied.
3. **Restructuring**: this is the case where workers' representatives wish to be informed about structural changes in the company, which may have an impact on employment and working conditions, within or outside the scope of a transfer of undertaking or a collective dismissal.
4. **Collective defence**: this is the case where trade union representatives wish to obtain information about human resources practices or about economic and financial issues related to a company, in light of initiating or conducting negotiations with the employer in order to defend the interests of their workers.
5. **Individual representation**: this is the case where workers' representatives are asked to represent an individual worker and wish to have access to information from the employer related to the individual.

d. Model-levels

Within each of the model scenarios of industrial relations where information exchange is required, four different levels of information exchange could be identified.

They could be seen as follows:

A (transnational) Information at the level of the **European Trade Union** organization (established in the sector)	**B (transnational)** Information at the level of the **European Works Council** (established in the context of the multinational company concerned)
C (national) Information at the level of the **national Trade Union** organization	**D (national)** Information at the level of the **national workers' representative body** (established in the context of the national company concerned)

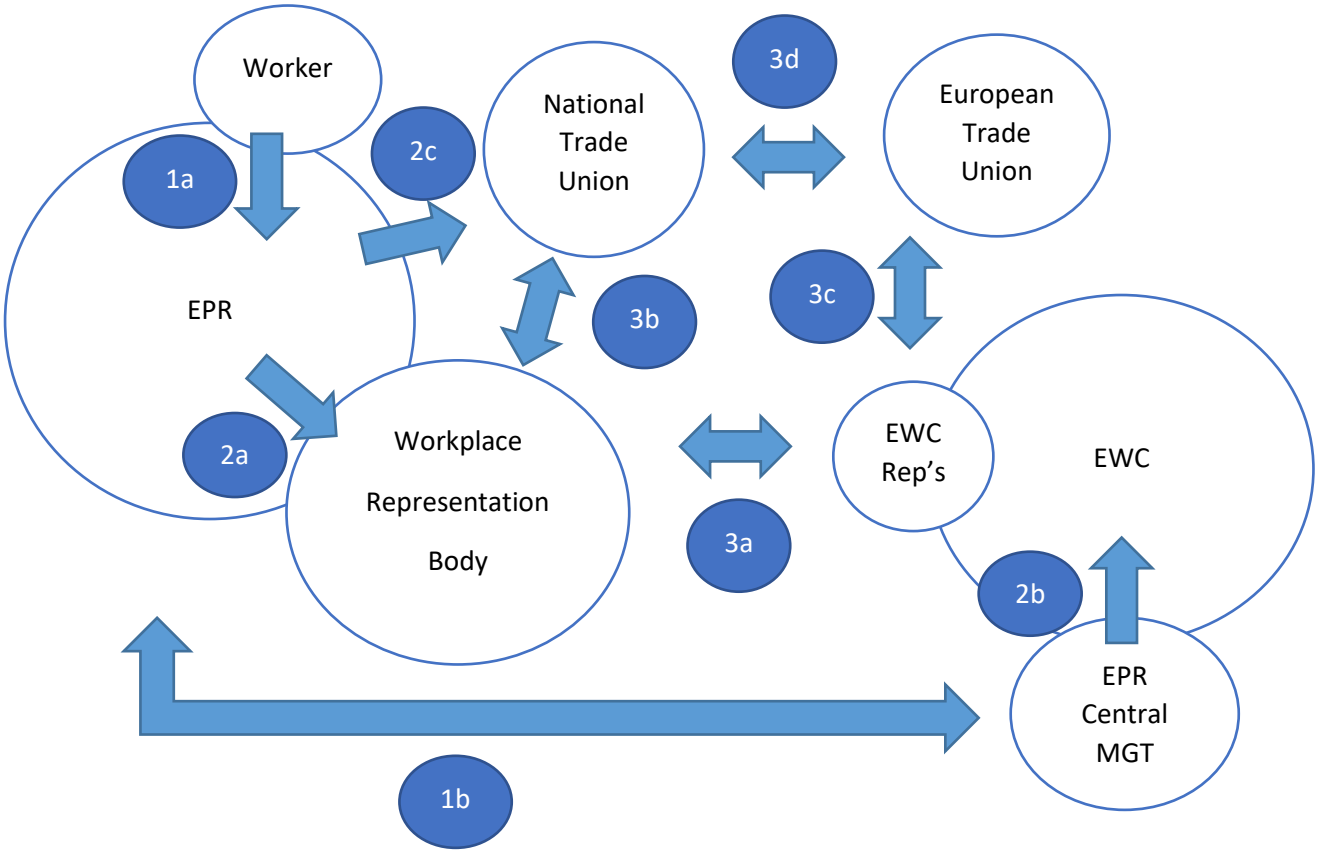
It is not unlikely that, for some of the model scenarios described above (cases 1-5) the most appropriate level may be a transnational (European) level of information, while for other the national level may be more effective.

There will be situations where national and transnational information will interfere with each other. This makes the impact on personal data protection obviously more complex.

e. Data flow chart

Hereafter, a **data flow chart** is provided. The flow chart represents potential (personal) data flows between different industrial relations actors. The actors are based on the model scenarios and levels, as well as on existing mechanisms industrial relations in a European, multinational, context.

Data flow chart:



The **arrows and numbers** indicate the flow of data. The following data flows can be identified:

- **1a:** data shared by workers with their employer in the context of human resources
- **1b:** HR related data shared between employers belonging to the same group of undertakings (e.g. subsidiary and headquarter)
- **2a:** data shared by the employer with the national workplace representative body (e.g. to the works council)
- **2b:** data shared by central management with the European workplace representative body (e.g. the European Works Council - EWC)
- **2c:** data shared by the employer with a national trade union organization
- **3a:** data shared between national workers' representatives with European (EWC) workers' representatives
- **3b:** data shared by national workers' representatives with a national trade union organization

- **3c:** data shared by European (EWC) workers' representatives with the European trade union organization (e.g. in the relevant sector, for the relevant profession)
- **3d:** data shared by a national trade union organization with the European trade union organization (e.g. in the relevant sector, for the relevant profession)

The flow chart represents the **complexity** of information flows in a more complex industrial relations setting. It also shows, for example, how data, which may have been originally collected by employers for HR purposes from their staff members, may subsequently be targeted for further use in workplace representation settings and even further for processing within the trade union movement. This will be discussed below.

The flow chart will be used to deliver an applied analysis of subsequent key toolbox-questions.

c. Key findings

Key points:

- ✓ Industrial relations cover a complex variety of systems and practices
- ✓ It is therefore important to identify data flows

Solutions:

- ✓ Establish a data flow chart
- ✓ Adapt the flow chart to the specificity the industrial relations context
- ✓ Use the data flow chart for applying of the subsequent toolbox questions

Q2: Who is identified as controller/processor/recipient ?

a. Analysis

In the context of this study, which relates to different actors and processes undertaken in (European-wide) industrial relations, it is important to identify the key responsible **actors** in terms of the GDPR.

The GDPR distinguishes the concepts of controller and processor. Article 4 of the GDPR gives the following definitions:

- **controller**: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

  Elements are:[172]
  - A controller determines the purposes and means of the processing, i.e. the why and how of the processing.

[172] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, p.3: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

- The controller must decide on both purposes and means. However, some more practical aspects of implementation ("non-essential means") can be left to the processor.
- It is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller.

- **processor**: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

  Elements are:[173]
  - A processor is a separate entity in relation to the controller.
  - It processes personal data on the controller's behalf.
  - The processor must not process the data otherwise than according to the controller's instructions (though the controller's instructions may leave a certain degree of discretion about technical and organisational means).
  - The processor does not determine its own purposes and means of the processing (as in that case, the processor will be considered a controller).

The EDPB has determined, in case of doubt or discussion, some factors of fact to indicate the difference between a controller and a processor:[174]

Factors that indicate that you are the controller	**Factors that indicate that you are the processor**
• You obtain a benefit from, or have an interest in, the processing (other than the mere payment for services received from another controller) • You make decisions about the individuals concerned as part of or as a result of the processing (e.g. the data subjects are your employees) • The processing activities can be considered as naturally attached to the role or activities of your entity (e.g. due to traditional roles or professional expertise) which entails responsibilities from a data protection point of view • The processing refers to your relation with the data subjects as employees, customers, members etc. • You have complete autonomy in deciding how the personal data is processed • You have entrusted the processing of personal data to an external organisation to process the personal data on your behalf	• You process the personal data for another party's purposes and in accordance with its documented instructions - you do not have a purpose of your own for the processing. • Another party monitors your processing activities in order to ensure that you comply with instructions and terms of contract. • You do not pursue your own purpose in the processing other than your own business interest to provide services. • You have been engaged for carrying out specific processing activities by someone who in turn has been engaged to process data on another party's behalf and on this party's documented instructions (you are a subprocessor)

Additionally, article 4 of the GDPR gives the following definitions:

- **recipient**: "a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not"

[173] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, p.3-4: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

[174] Table taken from: Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, p.50: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

- **third party**: "a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data".

To illustrate that a 'third party' may be referring to a relevant party with close connection in the HR processing activities, as is shown by the EDPB, which gives the following example of HR related personal data transferred within a group of companies to the parent company (the latter to be regarded as a third party, regardless of the fact that all companies are part of the same group):

> "Example: Company groups – parent company and subsidiaries Companies X and Y form part of the Group Z. Companies X and Y both process data about their respective employees for employee administration purposes. At one point, the parent company ZZ decides to request employee data from all subsidiaries in order to produce group wide statistics. When transferring data from companies X and Y to ZZ, the latter is to be regarded as a third party regardless of the fact that all companies are part of the same group. Company ZZ will be regarded as controller for its processing of the data for statistical purposes."[175]

In light of this example, it should be noted that there may, nevertheless, be 'joint controllership' within a group of undertakings (e.g. parent company together with subsidiary entities).

It may be challenging, in practice, to clearly distinguish controllers and/or processors in cases in which personal data are shared. The fact that personal data are shared and leading to a final result in which a form of cooperation between different parties, and even a legal obligation, is at hand, does not necessarily qualify two parties joint controllers. The EDPB gives the following example:

"It may be challenging, in practice, to clearly distinguish controllers and/or processors in cases in which personal data are shared. The fact that personal data are shared and leading to a final result in which a form of cooperation between different parties, and even a legal obligation, is at hand, does not necessarily qualify two parties joint controllers."

> "Transmission of employee data to tax authorities A company collects and processes personal data of its employees with the purpose of managing salaries, health insurances, etc. A law imposes an obligation on the company to send all data concerning salaries to the tax authorities, with a view to reinforce fiscal control. In this case, even though both the company and the tax authorities process the same data concerning salaries, the lack of jointly determined purposes and means with regard to this data processing will result in qualifying the two entities as two separate data controllers."[176]

Additionally, the EDPB's guidance makes clear that a processor is an entity or person who is acting "on behalf of" the controller, meaning serving someone else's interest and being called to implement the instructions given by the controller. It also implies that the processor cannot carry out processing for its own purpose(s).[177] It should also be pointed out that, in principle, "there is no limitation as to the type of entity that may assume the role of a controller but in practice it is usually the organisation as

[175] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, p.29: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

[176] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, p.24: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

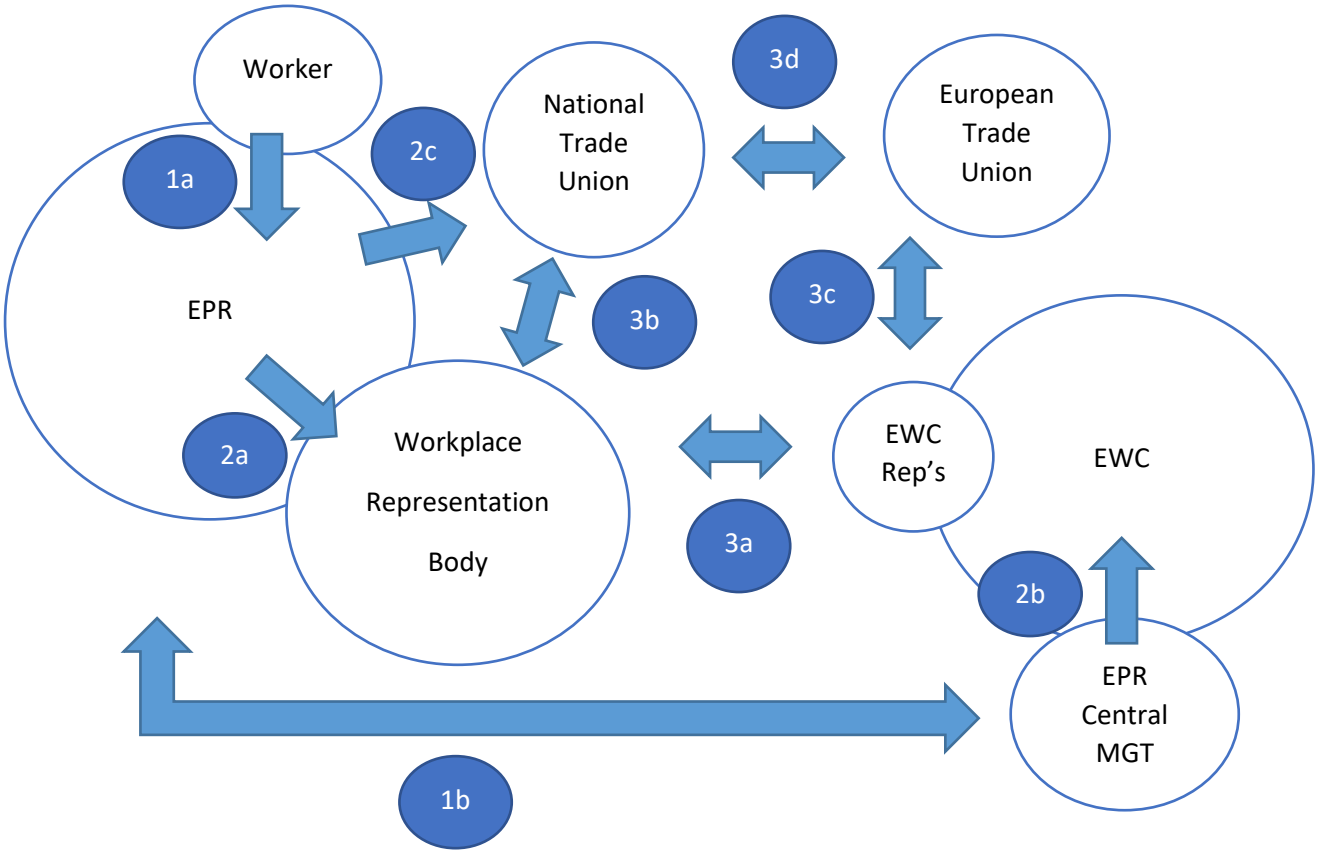
[177] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, p.26: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller."[178]

b. Application

Hereafter, we use the data flow chart to indicate how the responsible actors can be understood in terms of the GDPR.

Data flow chart:



For the GDPR, the notions of **controller**, **processor** and **recipient** can be explained below. The determination of the status of *controller* or *processor* will always be drawn from factual circumstances. In each scenario of industrial relations, a complex web of controllers, processors and recipients potentially arises. It should be stressed that the concepts are important to determine the rights and obligations of the involved parties and data subjects.

> "In each scenario of industrial relations, a complex web of controllers, processors and recipients potentially arises. The concepts are important to determine the rights and obligations of the involved parties and data subjects"

In light of the different scenarios, we departed from two main systems of workers' representation. On the one hand, we distinguish systems where representation goes through workplace representation

[178] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, p.3: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

bodies, such as works councils or employee representatives, and on the other hand representation through unions and/or union delegates. As indicated above, the reality may be more complex as industrial relations systems may mix elements of both.

On the basis of the above, in our view, the following positions can be determined:

- **Employer as controller:**

When, in an HR context, the employer collects personal data of staff members (1a), this employer will, as a rule, be considered as the controller of HR related personal data. The employer usually determines the *purposes* and *means* of the HR related data. The employer may rely on processors who process personal data on his behalf.

- **Employers as joint controllers:**

It may be that there is joint controllership between employers, meaning that more than one actor is involved in the data processing (and involved in the decision-making on 'the why and how' of the processing). This may be the case within a group of employers or a group of undertakings (1b).

The GDPR has specific rules on joint controllership and sets a framework to govern their relationship. This may be at hand in multinational corporate settings where HR data processing is determined by different entities within a group of undertakings (e.g. by a mother company in cooperation with other entities of the group). According to the EDPD's guidance, "an important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked".[179]

- **Trade union as controller:**

A trade union organization, national (2c) or European (3c,3d), which receives HR related data, from its delegates, representatives or from employers (of third parties), will have to be considered as a controller of the personal data concerned. A trade union organization may be strongly connected with the personal data processing of employers, to the extent that data are processed from their members or data are disclosed to trade union delegates. As a rule, trade unions will determine their own *purpose* and *means* of the personal data processing, also where it concerns data that they obtain as recipients, and will thus be engaged – as controllers – in their own data processing activities for the purposes of their trade union interests and that of their members.

- **Trade union as recipient:**

The potential position of 'controller' does not take away that a trade union, national (2c) or European (3c,3d), will be considered (also) as a recipient of personal data which they receive in the industrial relations context. In light of information (involving personal data) provided by employers, trade unions will be recipients of personal data, notwithstanding that they may become controllers themselves, or regardless of whether they are considered as third parties or not.

[179] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, p.3: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

- **Trade union (not) as a processor from the employer:**

Trade unions, national (2c) or European (3c,3d), determine their own *purpose and means* of the personal data processing which they receive, in relation to the purposes of their trade union interests and that of their members. These purposes are different (and may even be divergent) from those of the employer, even if the processing relates to the same HR personal data (as a result of disclosure by the employer to the trade union). A processor, on the other hand, operates under the instructions of a controller and does not determine its own purposes and means of the processing.

- **No joint controllership between trade unions and employers:**

While a 'collective governance' may be found behind the notion of industrial relations, we would not conclude that trade unions and employers are 'joint controllers' in the sense of the GDPR. Seen the different (or possible divergent) purposes of data processing, although taking place in a shared or even cooperative context of industrial relations, there is a more likely and sufficient separation between the own purposes and interests of trade unions and employers respectively in order to avoid any joint controllership between them, unless they would have explicitly defined a common framework of data processing, including a shared say over means and purposes.

- **Workers' representatives (not) as controller:**

The situation of workers' representatives (2a, 3b, 3a) is more complex and less obvious. A workers' representative may be an elected representative within a workplace representation body of the employer's company. The representative may either be a union or a non-union delegate. This may complicate the question who is a controller in the sense of the GDPR when the employer would give (personal data) information.

This qualification may be very case-specific. When workers' representatives receive personal data in light of their participation in workplace representation bodies (e.g. a works council), it is not obvious such individual members of bodies do not normally qualify as controllers. Whether the workplace representative body, as such, can be seen as a controller will not be evident either, since these bodies generally fall under the structures of the employer's company to which they belong, who may still mainly determine the means and purposes. The question, however, to what extent the employer has the final control over means and purposes of personal data, remains a question of fact and circumstances (see further on the application of the 'processor' concept).

It would also be difficult to qualify a trade union as a controller in this context, since workers' representatives may either be non-unionized, or may not be exercising their information functions as a trade union member, but as a workplace representative. Furthermore, if there is link between the workplace representative and the trade union to which he/she belongs, it may be (envisaged) that information is received and (subsequently) shared with the trade union, in which case both the workplace representative (who is a trade union member) and the trade union organization may become joint controllers. In short, the qualification will be highly dependent on the factual context and situation.

- **Workers' representatives (not) as processor:**

The situation of workers' representatives (2a, 3b, 3a), envisaged as a processor, is similarly less obvious. The question is, indeed, on whose behalf the workers' representative would be processing personal data. The context of industrial relations would seem to give the representative a *mixed* status. On the one hand, workers' representatives are part of workplace representation bodies within the context of the company's structures and obligations. Together with the employer, they build towards mutual relations and jointly realize the functions of these workplace representation bodies as defined by the applicable laws or agreements (2a, 2b). It may be the case that employers will pass on information (data) to representatives only for the purposes of fulfilling the obligation to provide information (and thus the right to information of the representatives). If the control over means and purposes remains in the hands of the employer, this may be an argument to qualify the representatives as processors of the personal data. On the other hand, the workers' representatives take part in these bodies on behalf of the workers which they represent and thus receive information from the employer for (arguably) other (and own defined) purposes and different interests than those defined by the employer. This might be an argument to disqualify them as processors of the employer.

Furthermore, it may also be questioned whether workers' representatives would be processors on behalf of the trade union to which they belong. It may be that enterprise-level workers' representatives are (depending on the system) not a trade union member, or represent the workforce and not the trade union, nor trade union members. This would give him/her a different function than a trade union (delegate), which may disqualify him/her as a processor of a trade union. At the same time, it may be (envisaged) that information is shared with the trade union to which a representative belongs (3b), in which case both the workplace representative (who is a trade union member) could become a processor of his/her trade union. In short, also here, the qualification may be highly dependent on the factual context and situation.

- **Workers' representatives as recipient:**

While it is an open question how a workers' representative (2a, 2b), elected in a workplace representation body, should exactly be qualified in terms of the GPDR (see above), he/she is recipient of information (provided by the employer), possibly including personal data. While it is difficult to indicate the controller for whom he/she is processing the information, the workers' representative will mostly be a recipient of personal data.

A simplified overview:

	Controller	**Processor**	**Recipient**
Employer	Yes, as holder of the HR data, determining *purpose* and *means* of the data	Only when he deals with personal data that he only processes and does not control (e.g. as part of a group of employers under the control of the headquarters)	Only if they receive information (personal data) from another controller, such as from another employer within a group, or from a trade union or workers' representative

	Controller	Processor	Recipient
Trade union	Yes, if recipient of the HR data, and determining *own purpose* and *means* of the data	Only when it deals with personal data that it only processes and does not control (e.g. as part of a larger trade union movement)	Yes, as recipient of HR data
Trade union delegate	No, the trade union for which the delegate acts will normally be seen as controller, unless they would qualify as joint controller with the trade union (depending on the situation)	Yes, they can be seen as processor on behalf of their trade union organization, unless they would qualify as joint controller with the trade union (depending on the situation)	Yes, as recipient of HR data
Workplace representative	No, they are normally not seen controllers, as they are individuals and member of a workplace representation body, although this cannot be excluded (depending on the situation). Who is (responsible) controller in this case, may remain unclear and dependent on facts and context (it may be the employer)	Yes, under circumstances they could be seen as processors on behalf of the employer (only). However, who is (responsible) controller in this case, may remain unclear and be dependent on facts and context	Yes, as recipient of HR data

c. Key findings

Key points:

- ✓ In any of the industrial relations scenarios, it is advisable to clarify the different roles and positions of all the actors in terms of the GDPR.
- ✓ Most unclear is the situation of individual representatives/union delegates
- ✓ GDPR obligations mainly rest on 'controllers' (who determine *purpose and means* of personal data processing)
- ✓ Two main controllers will be implied in industrial relations: employers (holding HR data) + trade union organizations (receiving HR data)
- ✓ *Individual* trade union delegates may qualify as 'processors' of their trade union organization. They also may be 'joint controller' with the trade union organization
- ✓ *Individual* workplace representatives are more difficult to qualify. This will be case specific. They could, depending on the situation, be seen as 'controller' or 'processor' in the sense of the GDPR

Solutions:

- ✓ Explicitly identify and document (e.g. in agreement with the employer), for each workers' representative or union delegate who may receive personal data in which capacity (controller, processor, recipient)
- ✓ Determine if a trade union organization may be involved in the data processing and, if any, whether it will function as a 'controller' (and identify the processors of this controller)

Q3: What is the legal/legitimate ground of personal data processing?

a. Analysis

As the GDPR requires that personal data processing should be justified on a legitimate/legal basis, it is important to assess and indicate the relevant legal ground for data processing by workers' representatives or trade unions in every specific case. As has been described in the analysis of the legal basis of information rights of workers' representatives in labour law, international and national legal sources will play a relevant role.

The following relevant legitimate grounds of processing are important in this industrial relations study:

1) Statutory obligations to provide information: the GDPR makes data processing legitimate "for compliance with a legal obligation to which the controller is subject". (art. 6, 1, c GDPR)

As indicated above, legal obligations arising from industrial relations law could constitute a possible legitimate ground of personal data processing. As discussed above, various obligations and rights require the exchange of information in industrial relations. If there is a legal obligation under industrial relations law to provide information to workers' representatives or trade union delegates, the disclosure of personal data can potentially be justified on that legal basis.

In Chapter 3, we have indicated that the data protection legal framework suggests some conditions for a legal basis to be valid as legitimate ground for processing. The GDPR's preamble mentions that the legal basis should be sufficiently "clear and precise" and its application should be foreseeable to persons subject to it.[180] Article 6, 3(b) of the GDPR provides that the purpose of the processing "shall be determined in that legal basis". As explained above, WP29 identified several requirements as regard to the notion "legal obligation",[181] including that the relevant law contains the requirement of necessity, proportionality and purpose limitation.

These conditions, as explained above, appear rather strict. From these, it would seem that, when rights regarding information and consultation of workers' representatives are applicable and require the exchange of information, the argument for *the need to also receive personal data* will need to be additionally made. This will be based on making the right to information more *effective*. That may place a certain *burden of proof* on the concerned parties (representatives, trade union, or the employer who may

"When rights regarding information and consultation of workers' representatives are applicable and require the exchange of information, the argument for *the need to also receive personal data* will need to be additionally made. This will be based on making the right to information more *effective*. That may place a certain *burden of proof* on the concerned parties (representatives, trade union, or the employer who may wish to disclose personal data)."

[180] Recital 41 Preamble GDPR.

[181] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 19-20.

wish to disclose personal data) to demonstrate a need of personal data.[182]

Our view is that the GDPR does *not* require that the relevant (labour) law needs to provide for an explicit mandate or permission to process *personal* data. When these conditions of *necessity* and *effectiveness* are met, there is room to disclose personal data under the relevant industrial relations legal provision.

2) Contractual obligation to process information: The GDPR makes data processing legitimate when justified "for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". (article 6, 1, b GDPR)

> "The employment context will give a broad justification in the employment context to process workers' personal data related to HR."

In the HR context, the processing of personal data is quite often based on processing which is necessary to perform contracts in the employment context. This will give a broad justification in the employment context to process workers' personal data related to HR, as relationships are in general based on agreements, either employment contracts or other contracts for work or services. Obviously, also here the condition is that the personal data processing should be *necessary*.[183]

3) Obligations arising from collective agreements: In chapter 3, we discussed collective agreements to which employers may be bound, as a ground for processing of personal data.

We see three possible angles:

a) Collective agreements could be seen as ***non-statutory legal obligations***. The GDPR's preamble mentions that, in order to establish a legal basis, it "*does not necessarily require a legislative act adopted by a parliament"* as long as "such a legal basis responds to the requirements of clarity, precision and foreseeability.[184]
Also collective agreements could, in our view, potentially constitute a legitimate ground of personal data processing. This will probably be the case for agreements that are binding to the parties under national law *and* which have been declared universally applicable.[185]

> "Collective agreements could constitute a legitimate ground of personal data processing. This will be the case for agreements which have been declared universally applicable."

b) From another perspective, collective agreements could constitute a ***contractual legal basis*** to the extent that they can be considered – in light of the GDPR – as a contract, of which the conclusion or performance may require the processing of personal data.

[182] This may be criticized, as the question whether personal data are really necessary (versus other data) is a question of proportionality/data minimization (see below).
[183] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 16.
[184] Recital 41 Preamble GDPR.
[185] See for this notion, Article 3.8, Posting of Workers Directive 96/71 of 16 December 1996.

However, this would rather justify the processing of personal data of the signatory parties to the (collective) agreement rather than third parties' personal data. The GDPR's provision is rather clear in requiring the only data can be processed related to parties to the contract. It is thus less evident for workers' representatives or unions to use the individual employment contractual basis to justify information of HR related personal data of workers.

"It is less evident for workers' representatives or unions to use the individual employment contractual basis to justify information of HR related personal data of workers."

c) As will be mentioned hereafter, the existence of a collective agreement may create a ***legitimate interest*** ground for personal data processing.
In the analysis of Chapter 3, it is indicated that, in article 88 of the GDPR, the European legislator recognises legitimate purposes, including "the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment" are acceptable, legitimate purposes of data processing. It also refers to "obligations laid down by collective agreements".
In our view, this means that the GDPR supports obligations and benefits arising from collective agreements as legitimate purposes of data processing.

"The existence of a collective agreement may create a legitimate interest ground for personal data processing."

4) Legitimate interests for data processing: Data protection standards, such as the GDPR (article 6, 1, f), show that personal data processing is not only legitimate when parties are *required* or *obliged* to process these data, based on legal obligations, but also in case where they have a contractual or other "legitimate interest".

From the analysis of Chapter 3, it is clear that such legitimate interest justifications may come from:

- employer's (business) interests
- interests of industrial relations
- public interest (e.g. health and safety)
- third party interests (e.g. interests of trade unions)

It should be noted that, when the data processing is based on the legitimate interests of the data controller or third parties, a balancing test has to be carried out. Interests of the data controller have to be balanced against interests or fundamental rights and freedoms of the data subject.[186] It is thus a rather dynamic and context dependent justification.

"Interests of the data controller have to be balanced against interests or rights of the data subject. It is thus a rather dynamic and context dependent justification."

[186] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 23.

5) Individual consent: The question is whether individual consent may be used as legitimate ground of processing. This may have a double aspect:

- Consent by workers given to own employer
- Consent by workers given to the trade union organization (of which worker is a member)

An additional legitimate basis for personal data processing could be obtaining consent, as a trade union, from the members of the trade union. As has been explained above, consent remains a *problematic ground* for processing and needs to meet certain specific conditions. Consent should therefore only be relied upon in last resort and to strengthen compliance with the GDPR.

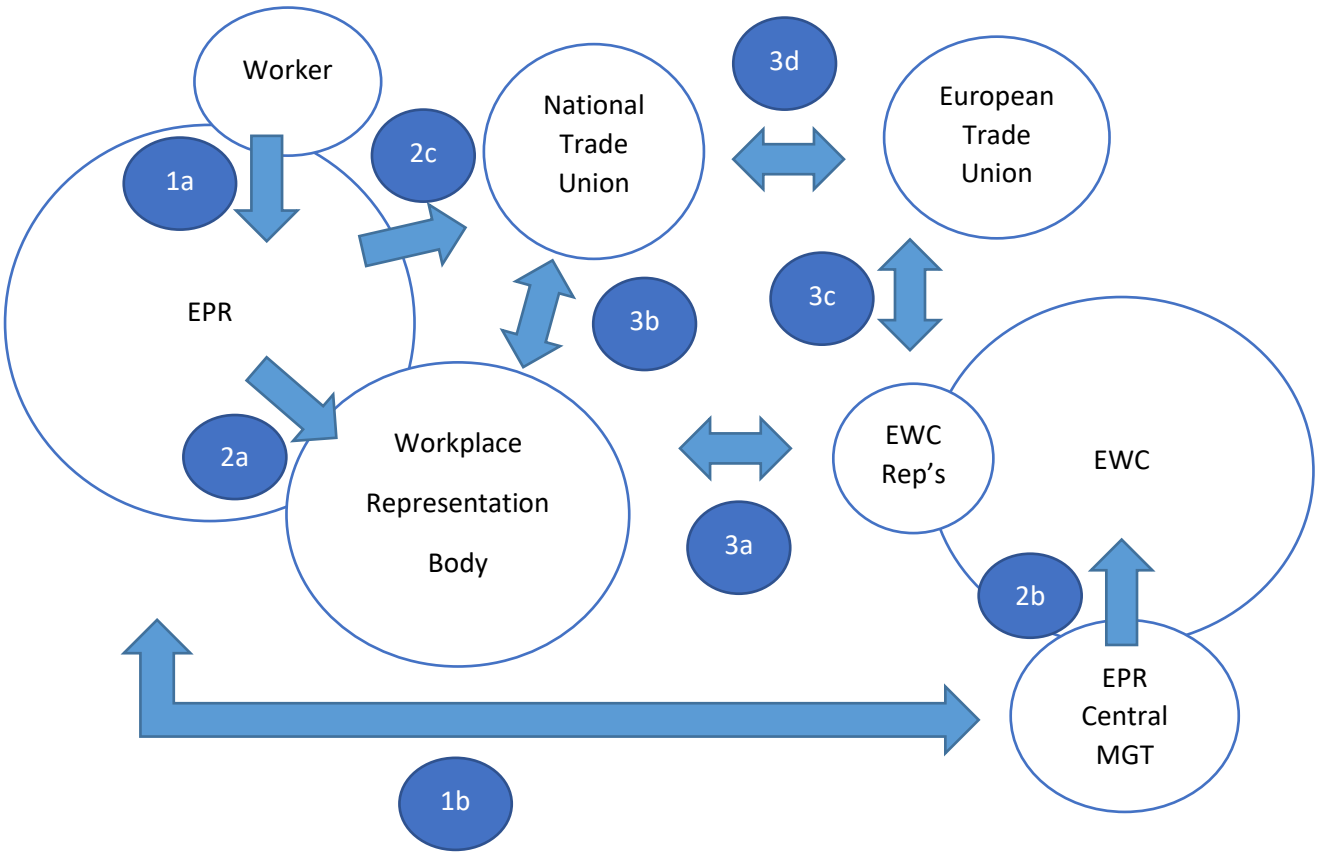
"Consent should only be relied upon in last resort."

Consent is not without problems. In light of improving compliance with the GDPR, a trade union may envisage to acquire consent from the individual trade union members. What could be envisaged is consent in light of trade union membership, whereby workers agree that certain personal data are shared and transferred between different trade union organizations (e.g. national and European trade union) for reasons of coordinating trade union activities and defending the interests of the members.

However, such consent would need to make clear that it is not merely about membership data, but also about HR data, which may be held by employers and which trade unions or their delegates may receive in a consultation or bargaining purposes. The safest way is that such consent is obtained individually, specifically and well-informed and documented, not as a standard clause in a trade union membership by-law for which members sign up. It may still be questioned whether this is a practical solution, since requiring individual consents is not easy to manage.

b. Application

Data flow chart:



Exchange of information in data flows:

- **Between individual employee and employer (1a) or group of employers (1b)** in HR or employment context:
    - **Relevant legal basis:** Statutory obligation, contract, legitimate interest

In order to establish an appropriate and well-functioning employment relationship, employees will have to share personal data with their employers. On the one hand, this is needed to fulfil legal rights and obligations in the field of employment law. In other words, employers will need to process personal data of employees to fulfill their legal obligations in employment (or e.g. tax) law. On the other hand, the processing of personal data of employees may also be necessary to fulfil contractual obligations following from the employment contract. These personal data will be given mostly by the employee him/herself, but employers may also create new personal data on employees (e.g. performance evaluations or information regarding their seniority). If the employment contract does not offer a sufficient basis, at least additionally the legitimate interest of the employer's business purposes and HR may be establish a legal basis.

- **Between employer and workplace representation body (2a):**
    - **Relevant legal basis:** Statutory obligation, legitimate interest

Different legal obligations regarding the information and consultation of workers' representatives will have to be fulfilled in order to establish the data flows between employers and workplace representation bodies. These **statutory obligations** will be found in national legislation whether or not they entail the transposition of the European directives providing specific information rights to workers' representatives. Therefore, the legitimate ground of the legal obligation will be applicable when this legislation requires informing the workers' representatives in occasions such as:

- Directive 2002/14 requires explicitly that workers' representatives are informed on the recent and probable development of (1) the activities and economic situation of the employer and (2) employment levels, anticipatory measures and threats within the undertaking. Information regarding (3) substantial changes in work organizations or contractual relations has to be provided as well.
- Legislation related to the restructuring of undertakings provides specific information rights to workers' representation bodies. In case of a collective dismissal, workers' representatives have to be informed on (1) the reasons of the collective dismissal, (2) the number and categories of workers affected by the dismissal, (3) the period in which the dismissals will take place, (4) the criteria for the selection of the workers and (5) the method for calculating any redundancy payments. In case of a transfer of undertaking, workers' representatives have to receive information on (1) the date or proposed date of the transfer, (2) the reasons for the transfer, (3) the legal, economic and social implications of the transfer for the employees and (4) any measures envisaged in relation to the employees.

Most of these *statutory* information rights are formulated very broadly. For instance, the requirement of informing workers' representatives of the legal, economic and social implications of the transfer of an undertaking for the employees may entail that information on certain employees have to be shared in the workplace representation body. As explained above, there will be a requirement to establish that certain personal data would be needed, based on the legal grounds, to realise the rights and obligations *effectively*.

The information rights in case of restructuring, provided by the European directives are rather broad but also contain a clear list of information that has to be communicated to workers' representatives. Therefore, also these information rights may be indicated as legal obligations for processing personal data. This will occur especially in case of collective dismissal, in which the employer has to provide the criteria for the selection of the workers. However, the question will be whether this information right also entails a legal obligation to provide the evaluation documents of these workers and the reasons why they have been selected for dismissal. One may argue that if this information is not provided, the workers' representatives will be not be to be consulted *effectively*.

The same question needs to be asked in the context of the transfer of undertaking. It is clear that the directive provides a legal obligation to deliver information on which pilots will be subject to the transfer and which actions will be undertaken for these pilots and the changes in their contracts. This information may be considered information on the legal and social implications of the transfer. However, it is unclear whether this information right does also entail a legal obligation for instance to share copies of employment contracts. That is why it will be important that trade unions and workers' representatives demonstrate that the access to these personal data is necessary to have meaningful consultations in case of restructuring.

Besides the transposition of these European directives, national legislation may also provide information rights to workers' representative bodies. This has been demonstrated by the German benchmark case, in which the court took into consideration whether or not the provisions on the

competence of the national works council may constitute legal obligations as legitimate grounds for the processing of personal data on employees. Therefore, if the works council needs personal information on employees in order to fulfil its legal competence and functions (for example to check whether the employer complies with the legal obligations in employment law), this may provide a legal obligation as legitimate ground for this processing of personal data.

Other legitimate grounds than fulfilling legal obligations in industrial relations seem to be less recommended, or not applicable. As mentioned above, it is highly unlikely that the legitimate ground of the performance of a contract applies in the context of industrial relations, because the GDPR requires that the data subject is a party of this contract.

However, the **legitimate interest** argument may always serve as a fallback option to justify the processing of personal data. In some cases, workplace representation bodies will have a legitimate interest to receive information, which may include personal data related to workers. This information will allow representatives to protect the interests of the workers more adequately and to fulfil their legal competences better.

As last resort, the **consent** of every worker can be obtained to exchange information in this data flow lawfully. Because of the requirements of consent in the GDPR, this legitimate ground is practically unfeasible.

- **Between central management and EWC (2b)**
    - **Relevant legal basis:** Statutory obligation, legitimate interest

It is rather unclear in the data flow between the central management and the EWC which exchange of information is required in order to fulfil the obligations in the EWC directive, because the EWC agreement will determine the scope and functions of the EWC and the procedures for information and consultation.[187] As mentioned above, the competence of the EWC is limited to transnational matters. This means that these matters have to concern 'the entire undertaking or group or at least two Member States'.[188] Moreover, the right to information on transnational matters of the EWC exist in the respect that it enable members of the EWC to acquaint themselves with the subject matter and to examine it.

The information rights and objective under the EWC Directive ('defining and implementing arrangements for information and consultation of employees in such a way as to ensure their *effectiveness* and to enable the undertaking or group of undertakings to take decisions *effectively*') will strengthen arguments to receive specific data, including personal data, in the absence of which information rights are no longer exercised effectively by EWC members. In support of this, justification of processing/disclosing personal data related to certain themes may be more robust, as the EWC directive provides a right to receive specific information when the subsidiary requirements apply. The EWC will have then the right to receive information on the situation and probable trend of employment, investments, and substantial changes concerning organisation, introduction of new working methods or production processes, transfers of production, mergers, cut-backs or closures of undertakings, establishments or important parts thereof, and collective redundancies.[189]

[187] Art. 5.3 and art. 6.2, c EWC Directive.
[188] Recital 16 EWC Directive.
[189] Annex I EWC Directive.

Also here, the **legitimate interest** argument may always serve as a fallback option to justify the processing of personal data. This legitimate interest argument will be strengthened, if the **EWC agreement** contains provisions on sharing specific data, including personal data, to the EWC members.

- **Between employer and national trade union (2c):**
    - **Relevant legal basis:** Statutory obligation, legitimate interest, (consent)

In the data flow between employers and national trade unions, it should be examined first whether there is a **statutory obligation** to exchange information in national employment law. European legislation refers only to 'workers' representatives' and do not address in general to trade unions. However, in some systems, there exists in some circumstances a right to bargaining between trade unions and employers. As discussed above, a right to bargaining may entail a right to exchange information in order to have meaningful negotiations. It also remains under discussion of union delegates are part of the workplace representation bodies, exercising information rights, or are rather bargaining partners. For example, French legislation provides explicitly some information rights for trade union delegates. Still, the question remains whether it implies a right to collective bargaining which also entails a right to receive specific data.

That is why, in most cases trade unions will have to demonstrate a **legitimate interest** in order to receive information on workers. As mentioned above, trade unions will have a legitimate interest because of their purpose and mission, and since negotiations with employers are undertaken to protect the interests of workers and to improve their working conditions.

Consent may be a useful element to make processing on behalf of the trade union more robust. With regard to the question whether trade unions may process personal data from workers who are also their members, individual **consent** (in light of union membership) could be a legitimate access point for processing as trade union. This would be restricted to the side of the *receiving* trade union (who starts a new data processing).

- **Between Workplace Representation Body and EWC (3a)**
    - **Relevant legal basis:** Statutory obligation, legitimate interest

Data flows between the workplace representation body and the EWC may be lawful on the legitimate ground of compliance with a **statutory obligation**. The EWC directive requires that information and consultation of the EWC is *linked* to those of the national workplace representation bodies.[190] The arrangements for these links need to be established and defined in such a way that they respect the competences and areas of action of the employee representation bodies. This provision remains rather vague and much will be dependent on the EWC arrangement. The statutory provision does not, in principle, give further specifics on possible information flows from the local representatives to the European works council. It will be a matter of discussion what is needed to make EWC rights *effective*.

Also here, the **legitimate interest** ground may be a fallback. Local and European representatives could have a legitimate interest to establish reciprocal data flows. But this case will need to be strongly build up, certainly if it implies a need for the involvement of personal data. What will more likely make the legitimate interest more robust, is an **EWC arrangement** whereby information flows (between local and European representatives) are specified and agreed upon.

[190] Art. 12 EWC Directive.

- **Between Workplace Representation Body and national trade union (3b)**
    - **Relevant legal basis:** legitimate interest, consent

Data flow between a workplace representation body and a national trade union, is less obvious. The existence of a statutory obligation to exchange information between these parties in national law is less evident. It would be more related to the practice and logic of industrial relations.

That is why a **legitimate interest** is more likely to be a relevant ground. Trade unions will have a legitimate interest because of their common purpose and mission. However, the exchange of information must be *necessary* to protect the interests of the members of the trade union.

Another ground to consider is **consent** from the workers. Consent is not easy and not without problems (see above). But a trade union may envisage consent in light of trade union membership, whereby workers agree that certain personal data are shared and transferred between different trade union *processors* and/or trade unions (e.g. union delegates and national trade union). It will, however, be challenging to organize and define the purposes and conditions to make this a sufficiently effective solution (if it does not prove to be effective, it will be problematic under the GDPR).

- **Between EWC and European Trade Union (3c)**
    - **Relevant legal basis:** legitimate interest

Also at European level, data flows between a the EWC and a European trade union, is less obvious. The existence of a statutory obligation to exchange information between these parties is less evident. The composition of EWC's is as diverse as industrial relations practice. Sometimes, EWC are supported by European trade union coordinators, who mainly assist the workers' (or union) representatives in the European works council, sometimes as an 'expert', sometimes without relying on a specific EWC statutory provision.

The EWC Recast Directive refers to European trade union coordinators, which receive, in order to enable them to monitor the establishment of new European Works Councils and promote best practices, the right to be informed of the commencement of negotiations.[191] However, their role in the actual functioning is less explicit.

That is why a **legitimate interest** is more likely to be a relevant ground. Trade unions will have a legitimate interest because of their common purpose and mission. However, the exchange of information must be *necessary* to protect the interests of the members of the trade union.

A key to making the legitimate interest basis more robust would be to include a European trade union representation in the functioning of the European Works Council and to include a mechanism in the EWC arrangement that certain information may be shared.

- **Between national trade union and European Trade Union (3d)**
    - **Relevant legal basis:** legitimate interest, consent

It is rather unlikely that statutory provisions could be considered of legal obligations to transmit personal data of workers between union organisations. For this reason, this data flow may be based mostly on the **legitimate interest** of the national trade union and/or the European trade union. For

[191] Recital 27, cf. Article 5,4 EWC Recast Directive 2009/38.

instance, the exchange of information may be *necessary* to protect the interests of the members of the national trade union.

Another ground to consider is **consent** from the workers. Consent is not easy and not without problems (see above). But a trade union may envisage consent in light of trade union membership, whereby workers agree that certain personal data are shared and transferred between different trade union organizations (e.g. national and European trade union). It will, however, be challenging to organize and define the purposes and conditions to make this a sufficiently effective solution (if it does not prove to be effective, it will be problematic under the GDPR).

c. Key findings

Key points:

- ✓ Legitimate interest and consent may be problematic / less secure grounds
- ✓ Employers' HR data processing will rely on : contractual obligations + legal obligations
- ✓ Sharing HR data in industrial relations will rely on: legal obligations, legitimate interest and (less on) consent

Solutions:

- ✓ Identify the legitimate ground for personal data processing: legal obligation, contractual basis, legitimate interest, consent
- ✓ European Works Council arrangements may make the legitimate ground more robust for data sharing with representatives (and possibly with trade union organizations)
- ✓ Trade unions may arrange consent from their members to allow HR data processing relating to them (if practical and effective)

Q4: Which (personal) data are communicated to the workers' representatives and for which purposes?

a. Analysis

In the analysis of Chapter 3, we identified the issue and importance of making sure that personal data are collected for specific (and legitimate) purposes, and that personal data are further used only for the same, original purposes, or for *compatible* purposes. Secondary use of personal data is, therefore, allowed.

However, we identified three scenario's (see above):

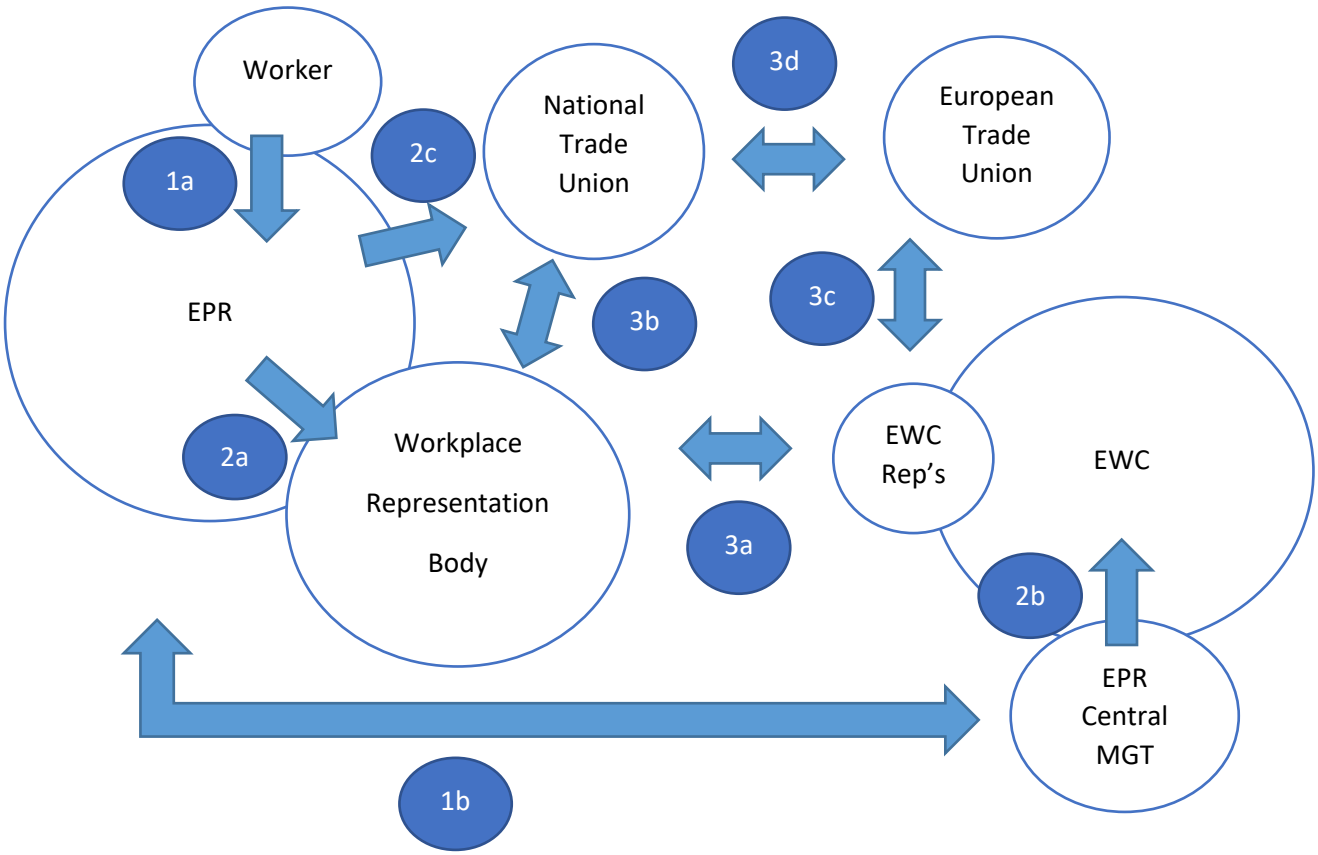
- *Scenario 1: Compatibility is prima facie obvious:* further processing of personal data may be found compatible, as "the processing clearly meets the reasonable expectations of the data subjects", even if not all details were fully expressed at the start.

- *Scenario 2: Compatibility is not obvious but still justified:* there is a 'connection' between the specified purpose and the way the data are subsequently processed. Either the purposes "are related but not fully matching", or data are further used "for different and not directly related" purposes, but their relationship or the context would still justified the secondary use. In this case, additional safeguards may be put in place in order to "compensate for the change of purpose (e.g. to provide additional information and explicit options for the data subject)".

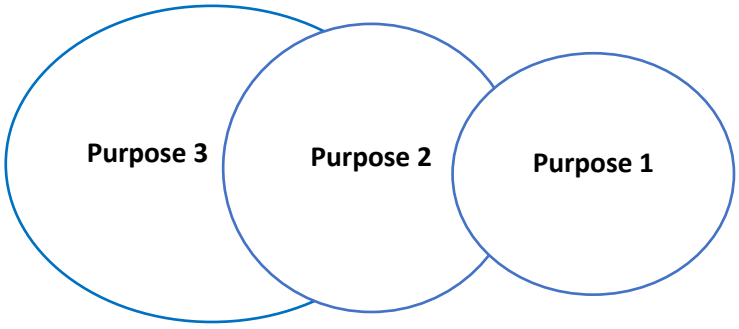
- *Scenario 3: Incompatibility is obvious:* It concerns the further use of data for additional purposes that a reasonable person would find "not only unexpected, but also obviously inappropriate or otherwise objectionable".

b. Application

Data flow chart:



In light of the data protection compatibility assessment, it is important to distinguish three different purpose-levels in the industrial relations data flow chart. This can be displayed as:



This is related to distinctive questions:

- **Purpose 1: for which (*original*) purposes have the personal data been collected in the HR context?**
- **Purpose 2: for which (*secondary*) purposes are the personal data communicated to the workers' representatives?**
- **Purpose 3: Can these personal data be involved in further (*tertiary*) purposes of data processing (e.g. processed by trade unions themselves)?**

The primary and **original purpose** of the personal data processing, at the stage of collection, will find its origin with the HR context of the employer. It must be assumed that the personal data will be collected and processed for a legal/legitimate basis of processing in the employers' HR context. There are also legitimate grounds (see above) to justify this.

➔ This will concern data flows 1a and 1b

Subsequently, the question of the **secondary purpose** of HR related personal data of workers relates to the purpose of communication those personal data to the workers' representatives. We established above our opinion that HR related data, collected by employers, can later (under further GDPR conditions) be used and shared with trade union delegates or workers' representatives in light of the exercise of rights and obligations in the context of industrial relations. This does not, in our view, qualify as incompatibility.

➔ This will concern data flows 2a, 2b and possibly 2c

A major problem will arise with regard to what we would call a **tertiary purpose** or use of HR related personal data of workers. This relates to the purposes of trade union organizations themselves. For example, a trade union who makes its own analysis, findings and determines its own policy steps, based on HR data received (sometimes not directly) from employers, will be much further away from the original purposes of collection of the HR context.

An aspect of the compatibility assessment is the interest of the data subject. An argument in light of this, to make the further processing still compatible with the original collection purpose is to point at the concern in employment related examples, which mostly show that the central concern is that workers' personal data are not used, in a later phase, against the legitimate interests of those workers. It could be argued that trade unions, per definition, will look for defending the interests of their members (workers). However, this does not necessarily compensate the weak connection between the tertiary purpose (trade union use) and the original purpose (employer's HR), nor gives a solution for non-members. Furthermore, an important dimension of re-purposing is that legitimate and reasonable expectations may play a role and whether data subjects could, fairly speaking, have been able to anticipate or foresee the new purpose.

An ideal solution does not seem to exist. Therefore, alternatives may be considered:

- it may be better to avoid personalized data in this phase and revert to **anonymized or pseudonymized** data instead.
- negotiate with employers and make sure that industrial relations purposes and further disclosure to trade unions are included in the ***original*** **purposes** of data processing (but this would require goodwill from employers)

Another alternative to search for a new legal ground of processing, connected with the new purpose, and related to this, reading the *tertiary* use as **a new personal data processing** activity, under the controllership of the trade union. The trade union may secure the legitimacy and purposes of this data processing on the basis of the explicit consent of its members (in the trade union membership relation). This obviously only relates to workers who are also union members. Furthermore, this solution would have an impact on the other toolbox-questions, such as Question 9, relating to risks of data subjects' rights and freedoms. Employers who are original controllers of the data may be reluctant to share data with unions, in order to minimize further risks, such as security problems, uncontrolled use, etc. It may, furthermore, be questioned, whether under article 6.4 GDPR, the employer, as original controller of the HR data, will not need to be implied in the consent of the workers concerned. Finally, there is the

view that, in case of incompatibility, it would not be possible to remedy this by "simply relying on a new legal basis".[192]

➔ This will concern data flows 3a, 3b, 3c and 3d

c. Key findings

Key points:

- ✓ HR personal data controlled by employers may be shared with workers' representatives and union delegates in light of their functions in workplace representative bodies. Such HR data sharing can be seen as a compatible but still justified (*secondary*) use of the data
- ✓ Further - *tertiary* - use of such HR personal data by trade unions for own trade union purposes (e.g. collecting data for analytical purposes) can be problematic under the purpose limitation principle. The connection with the original purpose of processing of the HR personal data looks insufficiently strong
- ✓ This will hamper the possibility for representatives or employers to share HR personal data with trade union organizations directly (for the trade union's own purposes)

Solutions:

- ✓ Solutions for *tertiary* use by trade unions may be: use anonymized/pseudonymized data and/or agree with employers to update the original purpose
- ✓ Another solution for *tertiary* use would be consent by the workers (concerned), though it leaves legal uncertainty (inherent to consent)
- ✓ Consent by a worker is more robust in a trade union membership relation, where the worker concerned seeks trade union representation in order to defend his/her interest in a particular case (this would be *secondary* use)

Q5: How is personal data processing minimized to what is necessary and proportionate?

a. Analysis

A central feature of data protection is data minimization. This implies that controllers should minimize the processing of personal data.

The principle is recognised in article 5, 1, c **GDPR**, providing that the processing of personal data should be:

> "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".

[192] Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203, 2 April 2013, p3; G. Verhenneman, *The patient, data protection and changing healthcare models*, Intersentia, 2021, p.294.

Avoiding or minimizing personal data also requires the consideration of alternatives, such as processing no data, or processing data only at anonymized levels. According to the European data protection authorities, "controllers should first of all determine whether they even need to process personal data for their relevant purposes. The controller should verify whether the relevant purposes can be achieved by processing less personal data, or having less detailed or aggregated personal data or without having to process personal data at all." [193] It is also pointed out that data minimization can also refer to the degree of identification: "If the purpose of the processing does not require the final set of data to refer to an identified or identifiable individual (such as in statistics), but the initial processing does (e.g. before data aggregation), then the controller shall delete or anonymize personal data as soon as identification is no longer needed. Or, if continued identification is needed for other processing activities, personal data should be pseudonymized to mitigate risks for the data subjects' rights."[194]

"Minimizing personal data also requires the consideration of alternatives, such as processing no data, or processing data only at anonymized levels".

Anonymization and pseudonymization are thus aspects to reduce the privacy impact or minimize personal data processing. It should be noted, along the GDPR's 26th Recital, that the principles of data protection do not apply to anonymous information, "namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".[195] Anonymization refers to making sure that individuals cannot be identified. Pseudonymization refers to rearranging or assigning the personal data to a pseudonym, like for example a code or number. This latter technique, in principle, would allow to trace back the individual's identity for those possessing the decoding information.[196]

Another dimension of this principle is storage limitation. The principle that personal data should not be kept or stored longer than necessary is connected to the data quality principle, but it can also be clustered within the proportionality principle.

"Another dimension of this principle is storage limitation. The principle that personal data should not be kept or stored longer than necessary."

The 'storage limitation' principle covers the idea that personal data need to be – and have to remain – relevant and cannot be processed for "longer than is necessary", seen the purposes for which the personal data are processed (cf. article 5, 1, e GDPR).

b. Application

Controllers should minimize the processing of personal data. For any of the model scenarios of industrial relations, the following issues will arise:

---

[193] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020, p.21, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[194] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020, p.21, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[195] Recital 26, GDPR.

[196] Cf. Working Party, Opinion 05/2014 on Anonymisation Techniques, Adopted on 10 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

- **Consider the first alternative: using aggregated (no personal) data**: while this should be the first reaction under the GDPR, this option is not always feasible in an industrial relations context.
  In many industrial relations cases, employers will give aggregated economic or social data, such as data on the company's performance, or aggregated personnel and employment data. The GDPR requires a demonstrated need for the disclosure of personal data. In practice, this necessity will be brought forward by trade unions or workplace representatives, based on the need to *effectively* exercise their collective labour rights. This need will follow from the case-specific context. For example, in a restructuring situation, the need to have information or a discussion on a *nominatim* list of (potentially affected) workers will need to be demonstrated, based on the specific industrial relations context. As long as this need is reasonably demonstrated, or agreed upon with the employer, there is leeway under the GDPR to disclose personal data.

- **Consider the second alternative: anonymize or pseudonymize data**: In some cases it may be an option to disclose anonymized or pseudonymized data. In light of the GDPR, this should be having preference over disclosing personal data. For example, if a certain HR practice is discussed (e.g. evolution or application of pay levels, discussion on holiday rostering) this could be considered. Names and identities of workers could be changed with numbers, codes or pseudonyms, and in this way disguised. In this situation, the personal data could remain with the employer while the anonymized/pseudonymized data are shared with the trade union delegates or workers' representatives.

- **Consider limiting the circle of data recipients**: In light of reconciling the need for personal data disclosure in industrial relations context on the one hand, and the data minimization principle under the GDPR on the other hand, limiting the number of data recipients should be considered. For example, representatives and employers could agree that, before disclosing data to workers' representatives, personal data will first be filtered by a limited group of data recipients. An option could be to establish a joint data protection body, including a representation from the employer and the workers. It would be advisable to also involve the data protection officer (DPO) of the employer.
  This body could have a filter function :
    - a place to decide on whether or not certain personal data will be disclosed to the plenary workers' representative body, or to a wider group of trade union delegates, weighing the effectiveness of industrial relations against the need for data protection.
    - a place to share and transform personal data into anonymized or pseudonymized personal data, which will then be shared in de-personalized form to the plenary workers' representative body, or to a wider group of trade union delegates.

- **Consider secure data disclosures**: In light of data minimization, and connected with the necessary **security risk** assessment (see further), consideration should be given to the question on which assets personal data will rely (oral information, paper and print formats, closed meetings, electronic forms, with or without data storage, etc.). This will determine the security levels of the data bearing format or platform.

c. Key findings

Key points:

- ✓ The GDPR requires a demonstrated need (*necessity*) for the disclosure of personal data
- ✓ In practice, this necessity will be brought forward by trade unions or workplace representatives, based on the need to *effectively* exercise their rights

Solutions:

- ✓ Anonymization or pseudonymization may be a feasible alternative for personal data processing: names and identities of workers could be changed with numbers, codes or pseudonyms, and in this way disguised
- ✓ An option is to leave personal data with the employer while anonymized/pseudonymized data are shared with trade union delegates or workers' representatives
- ✓ Consider the establishment of a joint body, including a representation from the employer and the workers, which has access to personal data and can filter (or anonymize/pseudonymize) personal data before disclosure in the broader industrial relations circle (compare with the 'select committee' in the EWC)
- ✓ Consider deleting (by e.g. aggregating/anonymizing/pseudonymizing) personal data immediately after they have been disclosed and have served the purposes of industrial relations

Q6: Have data subjects been informed ?

a. Analysis

A central aspect of data protection is the right of data subjects to be informed of a number of aspects, as mentioned in the GDPR. It requires transparency towards the data subjects concerned with regard to:

- identity and contact details of the controller and, where applicable, of the controller's representative
- contact details of the data protection officer, where applicable
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, including, if needed, with mentioning the legitimate interests pursued by the controller or by a third party
- the recipients or categories of recipients of the personal data, if any
- the fact that the controller intends to transfer personal data to a third country, with the relevant safeguards
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- the existence of the right to withdraw consent, where the processing is based on this
- the right to lodge a complaint with a supervisory authority

- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- the existence of automated decision-making, including profiling
- every relevant information in case the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, prior to that further processing

On the basis of this information or this transparency, data subjects can further exercise their rights under the GDPR (see below).

"Workers will have to be informed about all relevant aspects of data processing related to them as well as about their GDPR rights. This obligation rests on the 'controller'."

It implies that workers will have to be informed about all relevant aspects of data processing related to them as well as about their GDPR rights. This obligation rests on the 'controller'. It is thus very important to determine who is the controller of the personal data. In an HR context, this will primarily by the employer. However, as indicated above, also a trade union organization may become a controller of the personal data which it has received.

"Workers concerned should be informed about who receives personal data relating to them."

The GDPR requires, under articles 13 and 14, a controller to inform data subjects, not only about the data processing relating to them as well as the purposes of it, but also about the recipients or categories of recipients of the personal data. This means that the workers concerned should be informed about who receives personal data relating to them.

Following article 13, 3 GDPR and the GDPR's Recital, "where personal data can be legitimately disclosed to another recipient, the data subject should be informed [at the latest][197] when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information."[198] This means that if workers have not yet been informed and if new purposes are used to transfer of personal data to a new recipient (such as a trade union), the controller should inform the involved workers on beforehand.

"If workers have not yet been informed and if new purposes are used to transfer of personal data to a new recipient (such as a trade union), the controller should inform the involved workers on beforehand."

The exceptions to this duty of 'prior information' are rather limited and do not seem to apply to the industrial relations context envisaged in this study. It is provided that this obligation to provide prior information is not necessary "where the data subject already possesses the information" or "where the recording or disclosure of the personal data is expressly laid down by law" or "where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort".[199] Although information

"Anticipating to the obligation to provide information to the relevant data subjects (workers) whose data are disclosed will thus be important."

[197] Our addition.
[198] Recital 61 GDPR.
[199] Recital 62 GDPR.

(disclosure) to trade unions or representatives is laid down by law, the transfer of personal data concerning its workers by an employer is a consequence of obligations laid down by law in general terms (only) and may not be expressly laid down in the relevant legal sources.

Anticipating to the obligation to provide information to the relevant data subjects (workers) whose data are disclosed to trade unions will thus be important.

b. Application

In order to implement the rights to data subjects, it is important to indicate the relevant **controller**. With regard to the transparency requirement (giving information/notification to the data subject), the following situations may be envisaged. Above, we identified two main controllers in industrial relations, related to HR personal data: the employer and the trade union organization (potentially jointly with its delegates). More controllers may be identified, depending on the situation.

1. The **employer** will be the main controller of the HR personal data which may be disclosed to workers' representatives or the trade union (delegates). Regardless of IR, employers will have an existing obligation to inform the concerned workers about personal data processing, under his control, in the HR context (cf. flow chart 1a, 1b).

When the employer would disclose personal data to workers' representatives (2a, 2b) or a trade union (2c), the employer will need to **update and inform** the workers (as data subjects) about:

a) which personal data;
b) are disclosed to which new recipients;
c) for which new purposes
d) as well as "whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data" (article 13.3 j° 13.2.e GDPR).

The original purposes of data collection and prior existing transparency will be an important factor. It may be that the employer, as (original) controller, already informed extensively the workers (data subjects) concerned about the further processing, so that, as data subjects, the workers could have reasonably expect the further processing at the time (and in the context) of the collection of their personal data by the employer.[200]

We, however, assume that the most typical hypothesis is that HR personal data undergo a new (compatible) purpose and that the data subjects concerned have not yet (earlier) been informed about this.[201] In this case, according to article 13.3 GDPR, the employer/controller, who intends to further process the personal data for *a purpose other than that for which the personal data were collected*, must **provide the data subject *prior* to that further processing** with information on that other purpose and with any relevant further information (2a, 2b, 2c).

2. **Trade unions and/or workers' representatives** will be recipients of the information provided by the employer (2a, 2b, 2c).

The question hereby is:

a) whether these recipients will become (new) **controllers** (or processors of new controllers):

[200] Cf. Article 29 Working Party Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017 As last Revised and Adopted on 11 April 2018, p.23-24.
[201] It does not apply where and insofar as the data subject already has the information, cf. art. 13.4 GDPR.

b) whether, as controllers, they also need to **inform** the workers (data subjects) concerned. According to the GDPR, information to the data subjects is not necessary if the data subjects are already informed and/or if it would prove to be practicably impossible or involve a disproportionate effort;

c) and if not, how the rights and interests of data subjects will be guaranteed **otherwise**.

The issue under **a)** has been discussed under 'Question 2'. In principle, trade union organizations will be seen as (new) controllers when they receive personal data, since they determine their own purposes and means of the data processing involving those personal data. It cannot be excluded that workers' representatives are seen as part of the trade union's controllership (see above).

The question under **b)** is whether these controllers need to also give themselves information to the concerned workers when they receive personal data relating to them. For this issue, there is a relation with the obligations of the employer. If the employer already extensively provided the necessary information to the data subjects, it should not be repeated anymore.[202]

A problem here, in our view, is that the trade union or worker representative, receiving personal data may have another purpose or finality with regard to these data, perhaps involving new recipients. This should arguably be taken into account in order to evaluate whether new information needs to be given to the data subjects (workers) concerned. However, the recipient trade union/representative may not have the contact details of the data subjects (concerned). They could rely on the GDPR's exception that "the provision of such information proves impossible".[203]

However, if a trade union is pursuing its own objectives with HR personal data obtained from an employer, it will be difficult to dismiss this trade union from the GDPR's transparency obligations. Even in case of lack of contact details, European data protection authorities suggest that this does not necessarily dismisses a controller from its information duties, as it may give further information and transparency on its website.[204] Another way out is to jointly agree with the (original) controlling employer of the workers concerned to deliver the necessary transparency.

"If a trade union is pursuing its own objectives with HR personal data obtained from an employer, it will be difficult to dismiss this trade union from the GDPR's transparency obligations."

c. Key findings

Key points:

- ✓ Employers need to inform ('update') the workers concerned *on beforehand* when they disclose HR personal data related to them to unions/delegates/workers' representatives
- ✓ Trade union organization(s)/representatives need to inform the workers concerned when they receive personal data related to them, unless this information is already given (e.g. by the employer)

[202] Cf. article 14, 5, a) GDPR ("the data subject already has the information").
[203] Article 14, 5, b GDPR.
[204] Article 29 Working Party Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017 As last Revised and Adopted on 11 April 2018, p.29.

Solutions:

- ✓ Convince employers to include (preferably identified) workers' representatives as recipients of personal data in their transparency/information package towards their workforce (with specification of data and purposes)
- ✓ Agree with employers to jointly (employer + trade union) deliver the transparency/information package towards the workforce
- ✓ Give clarity on your trade union website and describe how you are GDPR compliant when HR personal data are received in light of industrial relations

Q7: What is the territorial scope of the personal data processing?

a. Analysis

The international sharing, disclosing or 'transferring' of personal data in an HR context is obviously an important dimension of the modern world of international business. It goes without saying that also within the context of human resources, international flows of data respond to a practical need. The *legitimacy* of sharing HR data within a group of undertakings, is (therefore) well recognized by the GDPR. Recital 48 of the GDPR reads:

> "Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected."

While the legitimate need for international data transfers is recognized, the GDPR however puts specific provisions and requirements in place. This is a rather complicated matter with an extensive range of issues.

Hereafter, we give an overview of the issues that play a central role. As not all of them may be practical for the purpose of information flows in light of industrial relations, we mainly point at the complexity of the issues as well as ways to avoid them. A balance needs to be struck between the need for personal data and the limits of international data flows, taking into account the proper functioning of industrial relations as envisaged in this study.

An important distinction needs to be made between the EU and the EEA[205] versus 'third countries'. The transfer of personal data to a *third country* is only legitimate if it is based on the conditions as outlined in the GDPR.

In the *Schrems II* case (C-311/18), the Court of Justice of the European Union (CJEU) has emphasised that the transfer of personal data to third countries cannot be a means to level down the protection afforded by the GDPR. The level of protection in third countries does not need to be identical, but it should be "essentially equivalent".[206] This should be taken into account when assessing the possibilities under the GDPR:

There are three main routes of providing this guarantee – they are seen as a 'cascade':

1) **Adequacy decision**: a transfer of personal data to a third country may take place where the European Commission has decided that an adequate level of protection can be assured in the third country or territory.

[205] European Economic Area: Norway, Iceland, Liechtenstein.
[206] CJEU, *Schrems (II)*, Case C-311/18, 16 July 2020.

So far, the European Commission has made adequacy decisions for:
Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United Kingdom[207].

The decisions are subject to specific conditions, meaning that generally relying on these decisions is not *per se* evident and further precaution should be taken. Additionally, the influence of the *Schrems II* case law might make some of them uncertain.

2) **Transfer tools**: in the absence of an 'adequacy decision pursuant', a controller or processor may transfer personal data to a third country if the controller or processor has provided appropriate safeguards, such as 'standard contractual clauses', 'corporate rules' or 'codes of conduct', pursuant to article 46 GDPR. In other words, private parties may organise specific transfer tools to guarantee sufficient protection of personal data when transferred to third countries.

The *Schrems II* judgment has created a rather high threshold. In order to assist exporters (e.g. data controllers, data processors), in assessing third countries and identifying appropriate supplementary measures where needed, the European Data Protection Board (EDPB) has adopted a series of recommendations. These recommendations provide a series of steps to be followed.[208]

Step 1: Know your transfers: this requires identifying and mapping all transfers of personal data to third countries. Being aware of where personal data go is necessary to ensure that it is afforded an essentially equivalent level of protection wherever it is processed.
Step 2: Verify the transfer tool: the GDPR lists the tools that can be used, such as standard clauses, codes of conducts, 'corporate rules'.
Step 3: Assess the third country: an assessment should be made whether there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards.
It should be noted, in this respect, that the EDPB has formulated a number of guarantees, called '*European Essential Guarantees*' that need to be in place in the third country legal system. These are:

- **Guarantee A -** Processing should be based on clear, precise and accessible rules
- **Guarantee B -** Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
- **Guarantee C** - An independent oversight mechanism should exist
- **Guarantee D** - Effective remedies need to be available to the individual

The EDPB, obviously, leaves the responsibility of the assessment and the weight of the different aspects to the responsible parties.
Step 4: Identify and adopt supplementary measures: this refers to measures necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. On 4 June 2021, the European Commission adopted a "Commission

[207] Commission Implementing Decision of 28 June 2021 on the adequate protection of personal data by the United Kingdom, Brussels, 28.6.2021 C(2021) 4800 final (https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf)
[208] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, 48p.

Implementing Decision"[209] with regard to standard contractual clauses, in order to guarantee sufficient levels of protection in light of the transfer of personal data to third countries pursuant to the GDPR. It provides a framework and a template, though the European Commission has stressed that every case is specific and parties should bear their own responsibility in addressing appropriate measures.

Step 5: **Determine formal steps**: the adoption of the supplementary measure(s) may require different initiatives or steps, depending on the transfer tool.

Step 6: Re-evaluate: at appropriate intervals the level of protection afforded to the personal data have to be monitored and re-assessed.

3) **Specific derogation**: The GDPR provides for derogations from what is provided and described above for international transfers of personal data. According to article 49 GDPR, international data transfers to third countries may be allowed under certain specific conditions. Some of these conditions seem to apply in the HR context, such as, for example, is the case where:
    a. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards, or
    b. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.

While this could cover HR related data transfers or personal data in light of the employment or industrial relation context, these GDPR derogations are seen as situations that need to be interpreted strictly and cannot relate to transfers within a 'stable relationship'.[210] Support for this restrictive view can be found in the GDPR's Recital 111 mentioning that the derogation can apply if "the transfer is *occasional* and necessary in relation to a contract".[211] This view is also followed by the European Data Protection Board (EDPB):

> "A transfer here may be deemed occasional for example if personal data of a sales manager, who in the context of his/her employment contract travels to different clients in third countries, are to be sent to those clients in order to arrange the meetings
>
> On the contrary, transfers would not qualify as "occasional" in a case where a multi-national company organises trainings in a training centre in a third country and systematically transfers the personal data of those employees that attend a training course (e.g. data such as name and job title, but potentially also dietary requirements or mobility restrictions). Data transfers regularly occurring within a stable relationship would be deemed as systematic and repeated, hence exceeding an "occasional" character. Consequently, in this case many data transfers within a business relationship may not be based on Article 49 (1) (b)".[212]

[209] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance)", C/2021/3972, *OJ L 199, 7.6.2021.*

[210] Ioannis Ntouvas, "Exporting personal data to EU-based IOs under the GDPR", *International Data Privacy Law* 2019, Vol. 9, No. 4, p281.

[211] Our emphasis.

[212] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 Adopted on 25 May 2018, p9, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

Furthermore, it can be questioned how practical individual (and unambiguous, explicit) consent would be, seen that international data flow is considered to be a particular data protection risk environment.[213]

b. Application

1. A balance needs to be struck between the information need involving personal data in an international context and the limits imposed by the GDPR on international data flows. This is mainly due to the specific conditions or restrictions put on the GDPR's regime related to 'third countries'.

2. The transfer to 'third countries' complicates the sharing of personal data in a human resources and industrial relations context. The GDPR requires that a proper level of protection remains guaranteed, equivalent to that of the GDPR. The main solution would be to create a proper 'transfer tool'. However, this is not a simple matter and should be carefully considered. Notwithstanding the European Commission's guidance, it obviously leads to rather complex solutions, seen the need to create specific transfer tools, such as standard contractual clauses.

3. An alternative – and advisable – solution is to avoid the transfer of personal data to third countries. We would suggest the following solutions :

a) Restrict international data transfers to import:
The specific requirements for international transfers of personal data are designed for *export* of personal data to third countries. Within the context of the industrial relations, as envisaged in this study, the needs for international transfer of personal data may be restricted to 'import of data' to the EU or EU recipients.

b) Restrict data transfers to EU/EEA only:
As the specific requirements for international transfers of personal data are designed for export of personal data to *third countries*, the industrial relations partners can (should) commit themselves to not transfer personal data outside the EU/EEA.
It is advisable that the industrial relations partners make an explicit arrangement (or agreement) whereby trade union delegates/worker representatives commit themselves to receive personal data only in the EU/EEA + on the condition that the personal data do not leave the EU/EEA.

c) Anonymize data:
The GDPR is not applicable to anonymize data. Depending on the needs for industrial relations purposes, the involved partners may decide to only engage in international transfers of *anonymize data* to third countries.

c. Key findings

Key points:

- ✓ International personal data flows to 'third countries' (outside EU/EEA) are severely conditioned by the GDPR

[213] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 Adopted on 25 May 2018, p6, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

- ✓ This leads to rather complex issues, certainly seen the context of potential industrial relations data flows
- ✓ Within the EU/EEA area, there are no further conditions, although some higher sensitivity for GDPR compliance should be respected

Solutions:

- ✓ Restrict data disclosures to recipients in EU/EEA only
- ✓ Anonymize data as much as possible when transferred outside EU/EEA

Q8: Are risks to the rights and freedoms of data subjects properly addressed ?

a. Analysis

When establishing complex networks or flows of personal data, and in order to strengthen compliance with data protection standards, the potential risks to the rights and freedoms of data subjects should be addressed and as much as possible diminished.

The obligations arising from the GDPR are related to the guarantee of rights to data subjects, mainly resting on the shoulders of the controller of the relevant personal data processing. However, where processing is to be carried out on behalf of a controller, the controller must use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.[214] Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.[215] It leads to a more collective or shared responsibility, with nevertheless a need to identify the different responsibilities and obligations.

The parties involved should give clarity to the following potential risks which can be identified and appropriate measures should be in place at the respective levels to secure data and the rights of data subjects:

1. **Risk that the rights of data subjects cannot be exercised**: The GDPR gives specific rights to all individuals whose personal data are processed (rights of data subjects):

- information provided to the data subject (Articles 12, 13 and 14 GDPR);
- right of access and to data portability (Articles 15 and 20 GDPR);
- right to rectification and to erasure (Articles 16, 17 and 19 GDPR);
- right to object and to restriction of processing (Article 18, 19 and 21 GDPR).

All measures must be taken that these rights can be effectively exercised.

2. **Security risks**: different kinds of risks are related to security of personal data processing activities. More specifically, risks include, illegitimate access, data leaks, undesired modification, disappearance personal data) from the perspective of the data subjects.[216]

[214] Article 28, 1 GDPR.
[215] Article 28, 1 GDPR.
[216] cf. Recital 90; article 35(7)(d) GDPR.

3. **Confidentiality and integrity**: Security not only refers to technological or organizational measures, but also to all persons involved in data processing. Processors involved and authorised to process personal data should have committed themselves to confidentiality (unless an appropriate statutory obligation of confidentiality applies).[217] The **ILO Code of Practice** provides, for example, in section 5.12. that "all persons, including employers, workers' representatives, employment agencies and workers, who have access to personal data, should be bound to a rule of confidentiality."

4. The GDPR also gives **awareness-raising and training** of staff, involved in processing operations, as examples of data compliance and risk prevention.[218] The **ILO Code of Practice** provides, for example, in section 5.9., that "persons who process personal data should be regularly trained to ensure an understanding of the data collection process and their role."

b. Application

1. As explained under 'Question 2', the data flows in an industrial relations context as envisaged in this study implies the involvement of different actors and roles of these actors may vary depending on the situation. Part of the data protection risk assessment will thus be to identify the different roles in terms of the GDPR concepts and notions. Mainly, the notions of 'controller' and 'processor' will play an important role, as most GDPR obligations are directed to these data protection actors.

We have clarified above that, in most intensive data exchange situations, two major personal data processing 'controllers' will be present: the employer and the trade union organization (alone or jointly with trade union delegates). We also mentioned a number of potential processors, such as workers' representatives or trade union delegates.

2. The controllers (employer and trade union organization) involved, need to guarantee that the **rights of data subjects** can be properly and effectively exercised. This requires procedures and mechanisms to make these rights effective (including, e.g., expertise and contact persons to deal with questions of data subjects).

3. With regard to **security risks**, not only the employer (as original HR data processor) but also trade union organizations who may later become recipients-controllers of the data will have to install the necessary technical and organizational measures to guarantee security of personal data.

4. Not only the employer (as original HR data processor), but also trade union members and representatives receive, or have access to, personal data need to have appropriate **awareness/training**.

c. Key findings

Key points:

- ✓ Attention needs to be paid to respect the rights of data subjects through all stages of data processing

Solutions:

[217] Article 28, 3, b) GDPR.
[218] Cf. article 39 and 47, 2, h) and n) GDPR.

- ✓ Trade unions are recommended to organise expertise to address issues related to the exercise of rights of data subjects (e.g. right to access, rectification, portability, …)
- ✓ Trade unions can contribute to technical and organizational measures to secure personal data
- ✓ Representatives and delegates need to live up to standards of integrity and confidentiality and need appropriate training
- ✓ Document compliance: make sure that there is documentation showing that all involved parties comply with data protection standards

Q9: Are additional guarantees applicable ?

a. Analysis

In order to contribute to a compliance culture in light of respecting the rights of data subjects in processing personal data and to facilitate the realization of industrial relations objectives, it may be proper to establish additional guarantees.

The GDPR itself offers a framework for – and in various cases even obliges – different tools for arranging compliance with GDPR standards. We are of the opinion that there is no strict obligation to establish or apply a specific tool described by the GDPR. Nevertheless, some suggestions can be made to improve and further document GDPR compliance and to pursue a joint strategy with employers.

The most relevant GDPR tools or strategies, in the context of this study, concerns

- standard contractual clauses (SCC);
- codes of conduct;
- collective bargaining solutions.

1. **SCC: standard contractual clauses**: these are contractual clauses ensuring appropriate data protection safeguards that can be used as a ground for data transfers. The European Commission has drafted 'model clauses' for:
    - **International data transfers to third countries:**
      See:
      - Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en
    - **Data transfers between controllers and processors:**
      See:
      - Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0915&from=EN
      - EDPB - EDPS Joint Opinion 1/2021 on the European Commission's Implementing Decision on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725,

https://edpb.europa.eu/sites/default/files/files/file1/edpb-edpsjointopinion01_2021_sccs_c_p_en.pdf

On the basis of the above analysis, our opinion is that the GDPR's **standard clauses** are, strictly speaking, not applicable (see further).

However, according to article 32, 4 GDPR, controllers and processors must take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law. This may require the establishment of **a documented practice of safeguards** before dealing, as natural persons, with receiving personal data.

2. **Codes of conduct**: voluntary accountability tools, whereby involved parties representing categories of controllers or processors translate and document their sector specific implementation and compliance with the GDPR.
   See:
   - Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 Adopted on 12 February 2019, p4, https://edpb.europa.eu/sites/default/files/consultation/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf

   The additional value of codes of conduct is explained by the EDPB:

   > "the GDPR introduces the principle of accountability, which places the onus on data controllers to be responsible for, and be able to demonstrate compliance with the Regulation. The provisions under Articles 40 and 41 of the GDPR in respect of codes of conduct ("codes") represent a practical, potentially cost effective and meaningful method to achieve greater levels of consistency of protection for data protection rights. Codes can act as a mechanism to demonstrate compliance with the GDPR. They also provide an opportunity for particular sectors to reflect upon common data processing activities and to agree to bespoke and practical data protection rules, which will meet the needs of the sector as well as the requirements of the GDPR."[219]

Codes of conduct are voluntary accountability tools, but they are strongly encouraged by article 40 of the GDPR.

3. **Bargained solutions**: In light of a joint effort to create a compliance culture in industrial relations and in order to address common concerns of employers and trade unions with regard to personal data processing, we would advise to envisage a bargained solution. This solution could be based on the standard clauses drafted by the European Commission, but it could also be reflecting the specific needs of the industrial relations partners and the specific sector needs.
   A bargained solution will more properly reflect the reality of industrial relations and will have different advantages. It also fits within the purpose of **article 88 GDPR**, which forwards solutions based on industrial relations for personal data protection issues in the human resources context (see further).

[219] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 Adopted on 12 February 2019, p4, https://edpb.europa.eu/sites/default/files/consultation/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf

A bargained solution may take different forms, such as a 'binding contractual clause' or as a jointly agreed 'code of conduct'. The bargained solution can be drafted for the specific purpose in one professional or company setting, but may also be a basis for talks about a *sector-wide* agreement.

b. Application

1. On the basis of the above analysis, the GDPR's **standard clauses** are in our view, strictly speaking, not applicable, since:

- Transfers of personal data to third countries (outside EU/EEA) would not be practical and should be avoided (see 'Question 7');
- The relationship between employers and trade unions is, as a rule, not a controller-processor relationship (but rather a relationship controller-recipient/controller) (see 'Question 2').

The tools can nevertheless be taken as both a source of inspiration and a benchmark of qualitative GDPR proof provisions.

However, according to article 32, 4 GDPR, controllers (and processors) must provide compliance instructions for any natural person – and this could be workers' representatives or trade union delegates – acting under the authority of the controller (or processor) and who has access to personal data. The natural person(s) concern should not process the data except on instructions from the controller.

2. An alternative may be to establish a **codes of conduct**. These instruments are voluntary accountability tools, encouraged by article 40 of the GDPR.

3. Although employers and trade unions are not *as such* joint controllers (see 'Question 2'), a joint initiative or a **bargained solution**, emanating from joint governance, is at least within the spirit of article 26 GDPR (referring to joint controllers, for which the GDPR obliges specific arrangements that reflect respective roles and responsibilities).

Advantages of a joint and bargained solution include:

- give expression to co-ownership of data protection concerns
- promotes trust and confidence in the sector
- shows (joint) consensus and reflects the needs of the involved actors in light of GDPR
- shows GDPR requirements that have been agreed as good practice within the relevant sector
- ensures that the involved actors are appropriately addressing the type of processing they are involved with
- defines roles and makes actors transparent and accountable

c. Key findings

Key points:

- ✓ Additional tools are strictly speaking not an obligation, but make data protection compliance more robust
- ✓ Additional tools increase legal certainty and mutual trust

Solutions:

- ✓ The use of standard clauses or codes of conduct are strongly advised

- ✓ Models are available from the GDPR framework
- ✓ A negotiated solution would strengthen the guarantees for different data flows within the multinational setting

Q10: Have interested parties been involved ?

a. Analysis

In assessing the different flows of personal data that may be envisaged, in light of the setting of this study, a final important question would refer to the involvement of the different actors and interested parties in the broader governance of data protection (standards). Where the involvement of interested parties seems to be a logical component of industrial relations, it is certainly an point of attention for strengthening data protection compliance. In addition, the GDPR includes a number of new institutions and actors, with the data protection officer (DPO) as a central figure.

"Where the involvement of interested parties seems to be a logical component of industrial relations, it is certainly an point of attention for strengthening data protection compliance."

1. Under the data protection framework, there is strong support a case for a **joint governance-approach** of data protection in an industrial relations context, whereby employers and trade unions or representatives jointly take up a collaborative strategy towards respecting the obligations of data subjects under the GDPR. This joint and collective governance, meaning the involvement of industrial relations parties, such as trade unions or workers' representatives, is suggested in different data protection sources.

The **ILO Code of Practice** particularly refers to it. According to section 5.11 of the ILO Code, employers, workers and their representatives should cooperate in protecting personal data and in developing policies on workers' privacy consistent with the principles in this code. Another dimension of this, is incorporating worker representative groups in data management and data protection impact assessment. It is referred to by section 12.2 of the ILO Code of Practice, mentioning that "***workers' representatives***, where they exist, and in conformity with national law and practice, should be informed and consulted" about certain aspects of data processing. Also section 5.8. of the ILO Code provides: "workers ***and their representatives*** should be kept informed of any data collection process, the rules that govern that process, and their rights."

The collective governance idea in the employment context has been explicitly suggested by the European data protection legislator in article 88 GDPR.

Article 88 of the **GDPR** provides:

> 1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.
>
> 2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

This implies that industrial relations becomes part of strengthening data protection solutions.

2. On the basis of the GDPR, the appointment of a **data protection officer (DPO)** is part of data protection obligations and guarantees, also in private companies or organisations. According to article 37 GDPR:

> "1. The controller and the processor shall designate a data protection officer in any case where:
>
> (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
>
> (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
>
> (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10."

This means that most private companies with large-scale data processing activities will need to appoint a DPO. The GDPR gives a central role to the DPO and has created, *de facto*, a new profession: an expert officer in an organization, who has the task, in an independent manner, to ensure that data protection law is applied, and who is a point of contact for information about personal data processing activities in the context of the organization concerned.[220] A group of undertakings may appoint a single data protection officer provided that he/she is easily accessible from each establishment.[221] The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.[222] He/she can thus either be an employee of the relevant undertaking, or an external or independent expert/consultant.[223]

Article 38 of the GDPR describes the position and role of the DPO:

> "1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
>
> 2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
>
> 3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.
>
> 4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.
>
> 5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
>
> 6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests."

b. Application

1. From the above analysis, the industrial relations scenarios and flow chart, it is clear that within the **context of industrial relations** envisaged in this study, there is a strong and rather sustainable link between controllers and (potential) various personal data recipients. This is not exceptional, as this

[220] P. Lambert, The Data Protection Officer. Profession, Rules and Role, Auerbach Publishers, 2016, 4.
[221] Article 37, 2 GDPR.
[222] Article 37, 6 GDPR.
[223] Cf. Recital 97 GDPR.

also exists broader in a network-societies or network-economies. However, in industrial relations, there are specific reasons for joint governance of data protection:

- there is a significant background of legal obligations with regard to information rights and obligations;
- there is existing potential for a collaborative environment, due to industrial relations practice with vested actors and structures;
- industrial relations actors, such as trade unions and representatives, largely represent the prime data subjects (workers) implied in the data processing activities
- there is a clear need for a culture of compliance with personal data protection standers.

2. In the industry underlying this study, the processing of personal data – including HR related personal data – will most likely occur with the involvement of a **Data Protection Officer (DPO)**. A group of undertakings may have a common/shared DPO.

In light of the exchange/disclosure of personal data in industrial relations between an undertaking and trade union/worker representatives, the involvement of the undertaking's DPO's is unavoidable. Seen the complexity – and the degree of sensitivity – of the involved data flows, also trade union organizations, becoming controllers of personal data, are recommended to appointment a own DPO.

The role of the DPO is predefined in the GDPR, but he/she may also fulfil "other tasks and duties" that are considered to be useful and effective in light of personal data protection standards. The DPO may be one of the actors in industrial relations performing various functions:

- consultation and advice with regard to the disclosure of personal data with industrial relations partners, in light of compliance questions or good practices within the context of GDPR (data protection impact assessment);
- be an intermediary and filter when selecting personal data for disclosure to industrial relations partners.

c. Key findings

Key points:

- ✓ Consultation on personal data processing activities and compliance should be part of good practice
- ✓ The employer's DPO (data protection officer) should be involved in joint consultations as well as in implementation of data processing activities

Solutions:

- ✓ Information and consultation on both HR and IR related data protection policies and practices with workers' representatives or trade union delegates is strongly advised
- ✓ Trade union organizations which become controllers of personal data are recommended to appoint a DPO (data protection officer) – the DPO may be operating under the umbrella of the European trade union organization

Conclusions, recommendations and toolbox

General

The main research aim and question in this study, was to find out as to what extent data protection laws and regulations (in particular the GDPR) can pose limits to the exercise of the right to information in a collective labour rights context where trade unions face employers or groups of employers in a transnational context. The analysis concentrated on data protection laws and principles, mainly departing from the perspective of the 'General Data Protection Regulation', known as the GDPR.

Chapter findings

In **Chapter 1**, we demonstrated that **the GDPR is a general instrument**, applying to a wide field of activities with a broad scope of application. It is necessary to adapt the rules and principles of the GDPR – like all general data protection standards – to the specificities of the employment context as well as to the field of industrial relations.

We also indicated that data protection standards rely on **fundamental rights frameworks**. It is, however, important to equally identify workers' and trade union rights as fundamental rights. This is key for two main reasons: 1) It may be necessary to reconcile different fundamental rights, as there is no general system of preference between these fundamental rights; 2) *framing* such rights discourse and conflicts involved may be crucial in legal assessments.

Chapter 2 elaborated the broader narrative and fundamental rights framework. We examined in more depth the conflict between information rights and the right to data protection. This is again important to **refine the *narrative*** of opposing rights and interest in an industrial relations context in light of GDPR concerns.

Theoretically, **data protection standards are not designed to *prohibit* data** or information flows. These standards rather engage in regulating and structuring the way how information is used or dealt with. There is no theoretical opposition between the right to information and the right to data protection.

The right to information and consultation is recognized as a fundamental right in Europe. The legislative (European/national) examples studied in this report indicate limits, including confidentiality, to information rights. However, the scope of confidential information, is subject to discussion. None of the examples give insight into whether personal data fall under confidential information as provided by industrial relations laws.

Two **benchmark cases show that data protection standards, such as the GDPR, do not stand in the way of disclosing personal data related to workers to the workers' representatives**. A European legislative proposal on equal pay allows individual pay data to be shared with workers' representatives. Arrangements can be made whereby disclosure individual pay information will be limited to the workers' representatives, not to individual workers. A German airline case confirms that information rights of works council representatives can be reconciled with the GDPR, even if it concerns sensitive information. An important requirement is that it must be shown that the information requested is indispensable to the performance of the task as a works council. But the general right to information contained in a statutory provision can justify the necessity of personal data processing.

Chapter 3 examined major GDPR principles of data protection, in light of justifying data disclosure in an employment and industrial relations context.

Three main and essential data protection principles are: Legitimacy; Proportionality; Purpose Limitation. On disclosure of personal data in an industrial relations context, there is – overall – few (to no) existing guidance. However, we are of the opinion that **information rights in industrial relations law may give a legal basis for the disclosure of personal data to workers' representatives**.

Data processing (including disclosure) should always be balanced with the rights of data subjects. Showing the ***necessity* to process personal data will be a crucial element**. This necessity may be derived from the need to be able to *effectively* exercise of the right to information.

The purpose limitation principle is probably the most difficult and problematic one to reconcile with the context of disclosing of information in industrial relations. This is related to the compatibility question: processing of personal data for purposes *other* than those for which the personal data were *originally* collected, is only allowed if this is *compatible* with the original collection purpose.

We are of the opinion that HR related data, collected by employers, can later be used and shared with workers' representatives. However, there will still be limits resulting from the GDPR and some secondary (or tertiary) use may be less obvious (as is shown and analysed in the final chapter).

Chapter 4 focused on making information and data exchange in industrial relations scenarios compliant with the GDPR and relate to the governance framework as well as tools for guiding data flows in industrial relations.

The whole **governance dimension is a highly relevant matter in finding solutions** for personal data protection problems and issues. The GDPR refers to various tools and mechanisms to secure that personal data processing is in conformity with the standards.

One of the means is a "data protection impact assessment" (DPIA), promoted as an important component of personal data protection. A DPIA is, as a rule, obliged for data processing with a 'high risk' impact or "likely to result in a high risk to the rights and freedoms of natural persons". In the context of our study, **we have applied the DPIA approach as a form of due diligence and good conduct** and as a way to create a culture of trust and compliance related to personal data protection, in particular the GDPR.

A number of related data protection impact questions, sufficiently practical for the industrial relations context of this study, have been narrowed down to **relevant key questions**. These questions should, in our view, be addressed when workers' representatives (or trade unions) and employers face issues of personal data in light of information disclosure in an industrial relations context :

1. What (personal) data flows can be identified ?
2. Who is identified as controller/processor/recipient ?
3. What is the legal/legitimate ground of personal data processing ?
4. Which (personal) data are processed for which purposes?
5. How is personal data processing minimized to what is necessary and proportionate?
6. Have data subjects been informed ?
7. What is the territorial scope of the personal data processing?
8. Are risks to the rights and freedoms of data subjects properly addressed ?
9. Are additional guarantees applicable ?
10. Have interested parties been involved ?

Recommendations and solutions

The **toolbox questions serve different purposes**. Not only do they provide the key elements for compliance, they also offer key points and recommendations. We also produced a data flow chart adapted to the industrial relations context.

The flow chart:

- ✓ is key to clarify accountability roles in terms of the GDPR with regard to the data flows involved
- ✓ represents potential (personal) data flows between different industrial relations actors. The actors are based on the model scenarios and levels, presented in this study, as well as on existing mechanisms of industrial relations in a European, multinational, context.
- ✓ is a reference for the application of the toolbox (with toolbox questions)

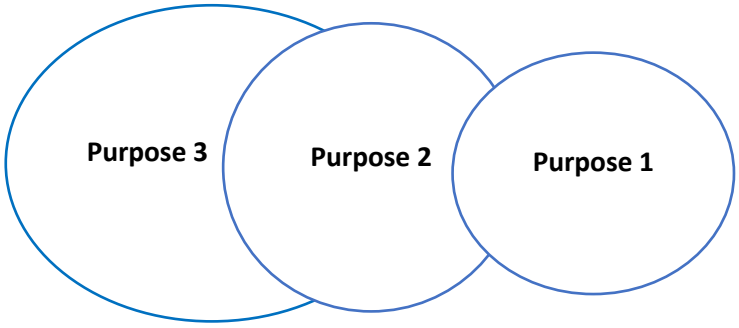
Toolbox:

- ✓ contains a series of recommendations for industrial relations partners, particularly workers' representatives and trade unions, in order to pursue GDPR compliance
- ✓ relies on what the GDPR requires in terms of data protection impact assessment (DPIA).
- ✓ is designed to meet the specificity of each particular industrial relations context

In an **Annex to this report**, we submitted a **Toolbox Chart** including the toolbox questions with guidance on key points and recommendations on solutions.

*

Based on the overall findings of this study and the tools mentioned above, a key problem arises within the context of the **purpose limitation** principle **and its connection to the legitimate basis** of various data flows. We identified three different purpose-levels in the industrial relations data flow chart. This can be displayed as:



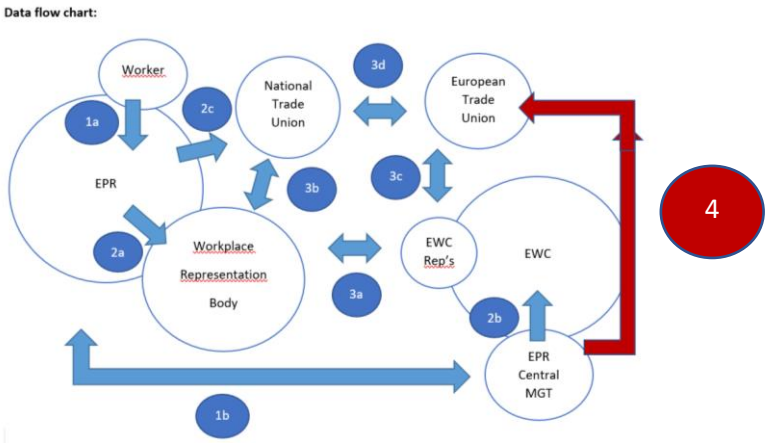
This is related to distinctive questions, understood as follows:

- Purpose 1: for which (*original*) purposes have the personal data been collected in the HR context? - Purpose 2: for which (*secondary*) purposes are the personal data communicated to the workers' representatives? - Purpose 3: Can these personal data be involved in further (*tertiary*) purposes of data processing (e.g. processed by trade unions themselves)?	- Purpose 1 is connected with data flows 1a and 1b - Purpose 2 is connected with data flows 2a, 2b and 2c - Purpose 3 is connected with data flows 3a, 3b, 3c and 3d

Purpose 1 and 2 have more robustness in terms of the GDPR's purpose limitation principle. Purpose 3, related to further trade union disclosure and use of personal data, should rather be defined as tertiary purpose and is less evident under the GDPR's purpose limitation principle.

A recommendation in this respect is to envisage a strong implementation of the other Toolbox questions in order to compensate the purpose limitation problem. In particular, in addition to options such as minimizing data processing (e.g. anonymization or pseudonymization) and limiting the circle of recipients, guarantees referred to under Question 9 can be recommended.

This may lead to adapting our data flow chart with the following addition:



The identification of a 4th relation in this chart, may have the following advantages:

- A negotiated agreement at European level with management and the European trade union
- Defining roles and accountability under the GDPR
- Adapted and uniform guarantees for GDPR compliance for the whole IR setting
- A stepping stone for a stronger legal basis of personal data processing and GDPR recognition
- A method to limit the circle of recipients of personal data

*

Our five key findings of the study:

- ✓ Personal data can be disclosed to workers' representatives in conformity with the GDPR
- ✓ In all cases, workers' representatives should demonstrate the *necessity* of personal data in order to be able to *effectively* exercise their right to information
- ✓ Data minimization is key, so maximize: anonymization, pseudonymization, limiting data access, and other safeguards
- ✓ Workers' representatives should use the Toolbox and Data Flow Chart in order to assess GDPR compliance
- ✓ Involve employers and reach agreement on conditions and standards applicable to HR personal data disclosures

* * *

Annex

Toolbox questions	Points of attention	Points of Actions / Solutions
1) Which (personal) data flows can be identified ?	- Industrial relations cover a complex variety of systems and practices	- Identify applicable data flows in an industrial relation context - Establish a data flow chart and adapt it to the specificity the industrial relations context - Use the data flow chart for applying of the subsequent toolbox questions
2) Who is identified as controller/ processor/ recipient ?	- GDPR obligations mainly rest on 'controllers' (who determine purpose and means of personal data processing) - Two main controllers will be implied in industrial relations: employers (holding HR data) and trade union organizations (receiving HR data) - Most unclear is the situation/role of individual representatives/union delegates o The qualification of individual workplace representatives will be case specific. They could, depending on the situation, be seen as 'controller' or 'processor' in the sense of the GDPR o Individual trade union delegates may qualify as 'processors' of their trade union organization. They also may be 'joint controller' with the trade union organization	- Clarify in any of the industrial relations scenarios the different roles and positions of all the actors in terms of the GDPR. - Determine if a trade union organization may be involved in the data processing and, if any, whether it will function as a 'controller' (and identify the processors of this controller) Explicitly identify and document (e.g. in agreement with the employer), for each workers' representative or union delegate who may receive personal data in which capacity (controller, processor, recipient)
3) What is the legal/legitimate ground of personal data processing?	- Employers' HR data processing will rely on the contractual obligations arising from the employment contract and the legal obligations in (employment) law - Sharing HR data in industrial relations will rely on legal obligations regarding information and consultation procedures, legitimate interests and (less on) consent - In industrial relations, legitimate practice may be more relevant than legislative frameworks - Legitimate interest and consent may be problematic / less secure grounds	- Identify the legitimate ground for personal data processing: legal obligation, contractual basis, legitimate interest or consent - Consider European Works Council arrangements to make the legitimate ground more robust for data sharing with representatives (and possibly with trade union organizations) - If practical and effective (and no other legitimate ground available), arrange consent from members of trade unions to allow HR data processing relating to them

Toolbox questions	Points of attention	Points of Actions / Solutions
4) Which (personal) data are communicated to the workers' representatives and for which purposes?	- HR personal data controlled by employers may be shared with workers' representatives and union delegates in light of the function of workplace representative bodies. Such HR data sharing can be seen as a compatible but still justified (secondary) use of the data - Tertiary use of these HR personal data by trade unions for own trade union purposes (e.g. collecting data for analytical purposes) may be problematic under the purpose limitation principle. The connection with the original purpose of processing of the HR personal data looks insufficiently strong. - This will seriously hamper the possibility for representatives or employers to share HR personal data with trade unions directly (for the trade union's own purposes) - Consent by a worker is more robust in a trade union membership relation, where the worker concerned seeks trade union representation in order to defend his/her interest in a particular case (this would be secondary use)	- Establish a compatibility assessment for secondary uses of HR personal data - Solutions for tertiary use by trade unions may be: ○ Use anonymized/ pseudonymized data ○ Agree with employers to update the original purpose ○ Arrange consent by the workers (concerned), though it leaves room for legal uncertainty (inherent to consent), and it leaves the question open who needs to receive the worker's consent (trade union or employer, or both)
5) How is personal data processing minimized to what is necessary and proportionate?	- The GDPR requires a demonstrated need (necessity) for the disclosure of personal data - Anonymization or pseudonymization may be a feasible alternative for personal data processing: names and identities of workers could be changed with numbers, codes or pseudonyms, and in this way disguised	- Necessity will be brought forward in practice by trade unions or workplace representatives, based on the need to effectively exercise their rights - An option is to leave personal data with the employer while anonymized/ pseudonymized data are shared with trade union delegates or workers' representatives - Consider the establishment of a joint body, including a representation from the employer and the workers, which has access to personal data and can filter (or anonymize/pseudonymize) personal data before disclosure in the broader industrial relations circle (compare with the 'select committee' in the EWC) - Consider deleting (by e.g. aggregating/anonymizing/pseudonymizing) personal data immediately after they have been disclosed and have served the purposes of industrial relations

Toolbox questions	Points of attention	Points of Actions / Solutions
6) Have data subjects been informed ?	- Employers need to inform ('update') the workers concerned on beforehand when they disclose HR personal data related to them to unions/delegates/workers' representatives - Trade union organization(s) need to inform the workers concerned when they receive personal data related to them, unless this information is already given (e.g. by the employer)	- Convince employers to include (preferably identified) trade union organizations as recipients of personal data in their transparency/information package towards their workforce (with specification of data and purposes) - Agree with employers to jointly (employer and trade union) deliver the transparency/information package towards the workforce - Give clarity on your trade union website and describe how you are GDPR compliant in case HR personal data are received in light of industrial relations
7) What is the territorial scope of the personal data processing?	- International personal data flows to 'third countries' (outside EU/EEA) are severely conditioned by the GDPR - This leads to rather complex solutions, certainly seen the context of potential industrial relations data flows - Within the EU/EEA area, there are no further conditions, although some higher sensitivity for GDPR compliance should be respected	- Restrict data disclosures to recipients in EU/EEA only - Anonymize data as much as possible when transferred outside EU/EEA
8) Are risks to the rights and freedoms of data subjects properly addressed?	- Representatives and delegates involved in data processing need to live up to standards of integrity and confidentiality and need appropriate training	- Trade unions who control personal data need to organise expertise to respond to questions and issues related to the exercise of rights of data subjects (e.g. right to access, rectification, portability, …) - Trade unions need to install technical and organizational measures to secure personal data - Make sure that there is documentation showing that all involved parties comply with data protection standards
9) Are additional guarantees applicable?	- Additional tools are strictly speaking not an obligation, but they can strengthen data protection compliance - Additional tools may increase legal certainty and mutual trust	- Consider to apply/negotiate models of standard clauses or codes of conduct available from the GDPR framework
10) Have interested parties been involved?	- Information and consultation on HR and IR related data protection policies and practices with workers' representatives or trade union delegates is strongly advised	- Involve the employer's data protection officer (DPO) in joint consultations as well as in implementation of data processing activities - Trade union organizations which become controllers of personal data are recommended to appoint a DPO - Consider whether the DPO may be operating under the umbrella of the European trade union organization