EMPLOYEE HEALTH DATA IN EUROPEAN LAW: PRIVACY IS (NOT) AN OPTION?

LENA ENQVIST* & YANA LITINS'KA†

While there are many feasible reasons for employers to process employee health data, the protection of such data is a fundamental issue for ensuring employee rights to privacy in the workplace. The sharing of health data within workplaces can lead to various consequences, such as losing a sense of privacy, stigmatisation, job insecurity and social dumping. At the European level, the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and EU General Data Protection Regulation (GDPR)–two interconnected instruments–offer the most enforceable protection of employee health data. The article analyses the limits of employees' right to privacy regarding health data, as delineated by the ECHR and GDPR. Using three fictive examples, we illustrate how the level of protection differs in these two instruments. In particular, we show that the protection of health data offered by the GDPR is seen as an objective act of processing at the time it is carried out, where the actual impact caused by the processing on private life is not considered. On the contrary, the ECHR's applicability and offered level of protection in the employment context depend on subjective factors, such as the consequences of sharing the data.

1 INTRODUCTION

Protection of health data at the workplace is a fundamental issue for many employees. Health data is intimate, sensitive and associated with risks if spread. Within workplaces, the sharing of such data can affect an employee's sense of dignity, lead to embarrassment, singling out, stigmatisation, job insecurity, social dumping and discrimination.[1] The sharing might also affect employees' relations with others in or outside the workplace and their general well-being.[2] On the other hand, an employer's obligations might include the necessity to process some of an employee's health data for various reasons, such as creating a safe work environment, complying with social security regulations, or ensuring the fulfilment of the

* LL.D., Assistant Professor specialising in Administrative Law at the Department of Law, Umeå University.
† LL.D., Researcher at the Department of Law, Lund University. Yana Litins'ka's research was financed by Sweden's innovation agency (Vinnova), dnr 2021-02648 and Lund University (internal funding for thematic collaboration initiatives).

[1] Eddie Keane, 'The GDPR and Employee's Privacy: Much Ado but Nothing New' (2018) 29 King's Law Journal 354, referencing Per Skedinger, Employment Protection Legislation: Evolution, Effects, Winners and Losers (Edward Elgar 2010); Megan Oaten, Richard J Stevenson and Trevor I Case, 'Disease Avoidance as a Functional Basis for Stigmatization' (2011) 366 Philosophical Transactions of the Royal Society B: Biological Sciences 3433; Leah S Fischer, Gordon Mansergh, Jonathan Lynch, and Scott Santibanez. 'Addressing Disease-Related Stigma During Infectious Disease Outbreaks' (2019) 13 Disaster Medicine and Public Health Preparedness 989.

[2] Sharyl Nass, Laura Levit, Lawrence O. Gostin, 'Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research' (*National Academies Press,* 2009) <http://www.ncbi.nlm.nih.gov/books/NBK9579/> accessed 28 April 2022.

employee's duties. Therefore, the right to privacy of health data in the workplace necessitates a sensitive and careful balancing between employer and employee interests.

The aim of this article is to analyse and compare the level of protection offered for employee health data in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[3] and the EU General Data Protection Regulation (GDPR).[4] These instruments have different applicational scopes, already evident from the fact that the scope of the ECHR comprises 46 Council of Europe Member States, while the scope of the GDPR is confined only to the 27 EU Member States.[5] The instruments are also addressed at different actors, where the ECHR is addressed to the states, and the GDPR, additionally, also is directly binding on those "controllers" who "process" particular personal data (here, the employers).[6] The GDPR is an implementation of Article 8—the right to data protection—of the Charter of Fundamental Rights of the European Union[7]. Yet, the GDPR's detail and scope go beyond the right to data protection in the Charter.[8] While there are differences between the ECHR and GDPR that affect the prospects of making clear-cut comparisons between these instruments, it is of great importance to study the level of protection provided by both of them. Within the EU, both instruments are simultaneously applicable. This means that the Member States, employees, employers and other stakeholders need to be cognizant of when and how the ECHR and GDPR protect health data and be able to navigate the differences in the protection provided.

In this article, our comparison will focus on how the ECHR and GDPR arrange and determine the level of protection to be offered for employee health data. To do this, we will structure our analysis around three fictive cases where health-related information is disclosed to an employer. The cases have been designed to represent situations where the ECHR and

---

[3] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) [1950].

[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) [2016] OJ L 119/1.
This article focuses on the level of protection each instrument offers in specific cases, which is here narrowly construed as relating to whether the particular employee health data may or may not be used by employers in these situations. The analysis does not, therefore, include other important aspects of the enforcement regimes of each instrument, such as the right to compensation or liability.
In this article we will refer to data protection as a part of the right to privacy, although the specific relations between the right to privacy and the right to data protection have been a topic of scholarly interest and debate. See, *e.g.* Orla Lynskey, 'Deconstructing Data Protection: The "added-value" of a Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569; Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental right?' in Ronald Leeds et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Cham, Springer 2017); Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222.

[5] Council of Europe, 'Map & Members', <https://www.coe.int/en/web/tbilisi/the-coe/objectives-and-missions#:~:text=It%20now%20has%2046%20member,%2C%20the%20Czech%20Republic%2C%20Slovakia%2C> accessed 15 June 2022; European Union, 'Country profiles', <https://european-union.europa.eu/principles-countries-history/country-profiles_en> accessed 15 June 2022.

[6] Article 1 ECHR; in the GDPR, obligations are placed on those who process personal data, whether private or state actors. The regulation also contains some obligations directly placed on the EU Member States, as well as a general obligation for them to make sure that their national legislation is GDPR compliant (see here, also, Article 36(4) for their obligation on prior consultation). Failure of a Member State to rectify violations of the GDPR could lead to the European Commission launching a formal infringement procedure under Article 258 TFEU.

[7] Charter of Fundamental Rights of the European Union [2000] OJ C 364.

[8] See section 3.1.

GDPR offer different levels of protection for employee health data and/or display differences in the interpretive steps they prescribe for assessing the permissibility of using or processing such data.[9]

In our first case, employee A is working from home due to the Covid-19 pandemic. A has tested positive for the virus, and the employer has a policy of disclosure regarding both positive and negative Covid-19 results. Although A is aware that no consequences are prescribed for incompliance, she discloses the test result to her employer.

In our second case, employee B has recently been diagnosed with bipolar disorder. B submits his medical certificate to the employer upon request to clarify the reasons for his recurring sickness absence. Shortly after, the employer e-mails all B's colleagues to inform them of the diagnosis, claiming that it will provide a safer working environment for all and psychological support to B. After the information is spread, B's colleagues avoid talking to him; B feels ostracized.

In our third case, employee C works as a nurse in a paediatric care department at a hospital and has recently been diagnosed with HIV. As required by national patient safety regulations applicable to C, she discloses this information to the employer. Shortly after, the employer decides to reallocate C to another department within the same hospital, stating that her infectious disease might risk co-workers' and patient safety in this particular working environment.

The cases of A–C each involve the exposure of an employee's health data to an employer or other external parties. However, they differ in terms of the type of disease and the consequences they incur. These differences will be discussed further to show how they affect the permissibility of employers' interference with employees' right to privacy in the workplace.

The article is structured as follows. In section 2, we will focus on the right to privacy for employees as established by the ECHR. Here, the European Court of Human Rights (ECtHR) case law will inform the analysis. In our reasoning, the Grand Chamber judgments will receive a more prominent role, but Chamber judgments and decisions will also be included.

In section 3, the provisions of the GDPR will be examined. This analysis will be based primarily on relevant legislation and the Court of Justice of the EU (CJEU) case law. Where these do not provide clear guidance, the opinions and guidelines of the Article 29 Working Party (Art. 29 WP) or the succeeding European Data Protection Board (EDPB) will be used.

We finish the article in section 4 with an overarching analysis of our findings, where we compare the different protection levels of employee health data that these instruments offer in cases A–C.

2 HEALTH DATA IN AN EMPLOYMENT CONTEXT: THE ECHR

2.1 PRIVATE LIFE AT WORK? DEFINITIONAL STAGE

We begin our analysis by highlighting Article 8 of the ECHR, which guarantees every person, including employees, the right to respect for private life. To assess whether a violation of the

[9] As opposed to the real-life cases resolved in a specific jurisdiction, the fictive examples here allow us to illustrate the reasoning of decision-makers in accordance with both the ECHR and GDPR.

right to privacy has taken place, the ECtHR must first establish that an interference with private life has occurred in a specific situation and that Article 8, therefore, is applicable.[10] If a case passes this definitional threshold of Article 8, the ECtHR will move on to assess whether the interference was justified. During this second stage, the ECtHR determines whether a state has violated the Convention. Our analysis in section 2.1 focuses on explaining the first step that the ECtHR takes in the assessment, the definitional stage. It answers whether Article 8 ECHR is applicable in situations where an employer requests an employee to provide health data, such as in cases A–C. After this (sections 2.2-2.4), we will proceed with the questions and problems raised at the second (justification) stage.

The ECtHR regards the term "private life" as broad and difficult to define.[11] Health data have long been considered a consistent part of "private life".[12] However, in an employment context, not every type of health data usage amounts to interference with private life. The ECtHR contemplates that privacy cannot always be reasonably expected in employment relations, implying an attempt to delineate private life and non-private relations.[13] These considerations are specific to employment relations and raise the threshold for applicability of Article 8 in these cases. In comparison, interference with private life occurs by default when health data is used in other spheres, such as in healthcare or by media. Nevertheless, the broad nature of private life renders Article 8 applicable in employment relations in two types of situations that may be interrelated. In these situations, the ECtHR uses either a so-called consequence-based or reason-based approach to determine the applicability. These approaches and situations are discussed below.[14]

The ECtHR would use the consequence-based approach in cases where an employer makes a decision that affects an employee's private life, to assess whether the consequences of the employer's decisions qualify as privacy interference. Examples include incidents when an employer's decisions impact the employee's reputation, opportunities to have relations with third persons, or where there are significant consequences for his or her individual "inner circle" (usually understood as a synonym for an applicant's family).[15] In cases where this approach is used, the ECtHR requires that the consequences reach a minimum level of severity. The minimum level of severity is an atypical requirement of the ECtHR jurisprudence on Article 8, yet it has been clearly established in the employment-related case

---

[10] See *e.g.* Janneke Gerards and Hanneke Senden. 'The Structure of Fundamental Rights and the European Court of Human Rights' (2009) 7 International Journal of Constitutional Law 619, 623.

[11] *Bărbulescu* v *Romania* [GC] App no 61496/08 (ECtHR, 5 September 2017), para 71; *Antović and Mirković* v *Montenegro* App no 70838/13 (ECtHR, 28 November 2017), para 41; *Sidabras and Džiautas* v *Lithuania* App no 55480/00 and 59330/00 (ECtHR, 27 July 2004), para 43; *Özpınar c Turquie* requête no 20999/04 (ECtHR, 19 October 2010), para 45; *Denisov* v *Ukraine* [GC] App no 76639/11 (ECtHR, 25 September 2018), para 95.

[12] See *e.g. M.S.* v *Sweden* App no 74/1996/693/885 (ECtHR, 27 August 1997), para 35.

[13] See *e.g. Bărbulescu* v *Romania* [GC] App no 61496/08 (ECtHR, 5 September 2017), para 73; Antović and Mirković v *Montenegro* App no 70838/13 (ECtHR, 28 November 2017), para 43; Joe Atkinson, 'Workplace Monitoring and the Right to Private Life at Work' (2018) 81 (4) The Modern Law Review 694, 697.

[14] *López Ribalda and Others* v *Spain* [GC] App no 1874/13 and 8567/13 (ECtHR, 17 October 2019), para 88; *Fernández Martínez* v *Spain* [GC] App no 56030/07 (ECtHR, 12 June 2014), para 110; *Özpınar* c *Turquie* requête no 20999/04 (ECtHR, 19 October 2010), para 45; *Denisov* v *Ukraine* [GC] App no 76639/11 (ECtHR, 25 September 2018), para 100.

[15] *Fernández Martínez* v *Spain* [GC] App no 56030/07 (ECtHR, 12 June 2014), para 110; *Oleksandr Volkov* v *Ukraine* App no 21722/11 (ECtHR, 9 January 2013), para 166; *Bigaeva* c *Grèce* requête no 26713/05 (ECtHR, 28 May 2009), para 24; *Denisov* v *Ukraine* [GC] App no 76639/11 (ECtHR, 25 September 2018), para 107; *Jankauskas* v *Lithuania (no 2)* App no 50446/09 (ECtHR, 27 June 2017), para 56; *Niemietz* v *Germany* App no 13710/88 (ECtHR, 16 December 1992), para 28.

law where the consequences-based approach is used.[16] The requirement means that applicants must identify and explain the significance of the effects of the employer's decisions on their private life, including the nature and the extent of their suffering resulting from the decision.[17]

How severe the ECtHR regards the consequences of a particular health data disclosure is context-dependent. For example, the attitude towards disease in a specific society can be one such factor that influences reputation, opportunities to have relations with others and can have consequences for the "inner circle". Such attitudes are likely to differ across Europe and from one workplace to another. They may also change over time and depend on scientific knowledge about the disease. Stigmatisation and significant consequences for individuals' private life may, similarly, depend on other, already inherent factors in each case, such as ethnicity – or factors external to the applicant, like the manner and context in which the information was shared.[18]

The consequence-based approach can be typically relevant when an employment-related decision makes others aware of sensitive data regarding employees. The case of B, where sharing information about the employee's mental disorder resulted in the ostracization of B, falls under this description. If the consequences were not as severe or could not be confirmed, the consequence-based approach would not apply. Compared to the case of B, there are no known consequences for A's private life as a result of her Covid-19 status disclosure. For C, the consequences—reallocation due to HIV—clearly exist. However, they are not directly related to C's private life, and it is unclear whether the threshold of severity will be reached. Therefore, the case of A and C is unlikely to reach the minimum level of severity threshold, at least so far.

The second type of situation where Article 8 can be impugned within employment relations is when an employer makes decisions based on *reasons* that concern a person's private life. Typical examples of relevant situations include not considering employees for promotion or dismissing them from work due to circumstances directly related to their private life, such as having a particular disease.[19] In such situations, the ECtHR uses the reason-based approach to determine whether there has been an interference.[20] In contrast to

---

[16] The requirement to prove that this minimum level of severity has been reached, for instance, is not clearly stated in case law where health data are shared by healthcare services. However, this requirement also exists in environmental case law. *L.H.* v *Latvia* App no 52019/07 (ECtHR, 29 April 2014), para 33; *Z* v *Finland* App no 22009/93 (ECtHR; 25 February 1997), para 70; *M.S.* v *Sweden* App no 74/1996/693/885 (ECtHR, 27 August 1997), para 35; *Mockutė* v *Lithuania* App no 66490/09 (ECtHR, 27 February 2018), paras 94–95; *Çiçek and others* v *Turkey* App no 44837/07 (ECtHR, 4 February 2020), paras 22, 29; *Fadeyeva* v *Russia* App no 55723/00 (ECtHR, 9 June 2005), para 69.

[17] *Denisov* v *Ukraine* [GC] App no 76639/11 (ECtHR, 25 September 2018), paras 110, 116–117; *Gillberg* v *Sweden* [GC] App no 41723/06 (ECtHR, 3 April 2012), para 73; *J.B. and Others* v *Hungary* App no 45434/12, 45438/12 and 375/13 (ECtHR, 27 November 2018), paras 128–129; *Gražulevičiūtė v. Lithuania*, App no 53176/17 (ECtHR, 14 December 2021), paras 99–100, 102–111.

[18] For example, in the beginning of Covid-19 pandemic it has been considered that persons of Asian descent were more stigmatised. Hyunyi Cho and others 'Testing Three Explanations for Stigmatization of People of Asian Descent during COVID-19: Maladaptive Coping, Biased Media Use, or Racial Prejudice?' (2021) 26 (1) Ethnicity & Health 94, 95.

[19] *Smith and Grady* v *the United Kingdom* App no 33985/96 and 33986/96 (ECtHR, 27 September 1999) paras 70–71; *Özpınar* c *Turquie* requête no 20999/04 (ECtHR, 19 October 2010), para 43.

[20] *Denisov* v *Ukraine* [GC] App no 76639/11 (ECtHR, 25 September 2018), paras 102–108; *Polyakh and Others* v *Ukraine* App no 58812/15, 53217/16, 59099/16 and 23231/18 (ECtHR, 17 October 2019), para 205; *Pişkin* v *Turkey* App no 33399/18 (ECtHR, 15 December 2020) para 176.

the consequences-based approach, here, the ECtHR does not require that a minimum level of severity must be reached.[21]

The case of C serves as a typical example of when the reason-based approach can be used. C was reallocated or not allowed to perform specific assignments due to her HIV, a circumstance directly related to her private life. Conversely, the employers of A and B have not made employment-related decisions.

To summarise, the definitional threshold for Article 8 will be met when employment-related decisions lead to significant consequences for an employee's private life (consequence-based approach) or are connected with a disease that an employee had (reason-based approach). This reasoning means that the consequence- and reason-based approaches can be relevant in B's and C's cases. The studied case law does not draw any relevant distinction for passing the definitional threshold depending on whether the data processing is imposed by national law (as in C's case) or conducted on request (as in B's case) for the applicability of Article 8.

In the case of A, the obligation to report Covid-19 test results has neither led to any employment-related consequences nor any yet known significant adverse effects on A's private life. The mere act of requesting data about a disease or the existence of a policy at the workplace does not signify interference with the right to privacy in the area of employment. This conclusion stands until there are no consequences for A that reach the minimum level of severity or the employer makes decisions based on A's diagnosis. The potential stigmatising effects of the disclosure are of no relevance. Therefore, A's case is unlikely to amount to an interference with the right to privacy under Article 8 ECHR, and will therefore not be discussed any further in section 2.

2.2 JUSTIFICATION STAGE: IDENTIFYING THE QUESTIONS

If the ECtHR finds that an interference with a person's private life occurred, it turns to the justification stage of the assessment. During this stage, the ECtHR evaluates whether a state has breached its duty not to interfere or failed to act to ensure the effective realisation of the right. A violation of the duty not to interfere is referred to as a breach of the state's *negative obligations*; a failure to act is categorised as a violation of *positive obligations*.

In cases concerning data usage in employment, the ECtHR has taken a relatively simple approach for distinguishing between the duty not to interfere and the obligation to act. If the employer is a state authority or company linked to the state, the duties not to interfere (negative obligations) are discussed.[22] When an alleged violation concerns the actions of a private entity, the ECtHR concludes that issues regarding the fulfilment of duties to act (positive obligations) arise if the national courts have accepted the private entities' interference with personal life.[23] Therefore, depending on whether the employer is a public

[21] *Gražulevičiūtė v. Lithuania*, App no 53176/17 (ECtHR, 14 December 2021), paras 98–99.
[22] *Libert* v *France* App no 588/13 (ECtHR, 22 February 2018), para 38; *Bigaeva* c *Grèce* requête no 26713/05 (ECtHR, 28 May 2009), para 31; *Gillberg* v *Sweden* [GC] App no 41723/06 (ECtHR, 3 April 2012), para 64; *Vukota-Bojić* v *Switzerland* App no 61838/10 (ECtHR, 18 October 2016), para 47.
[23] *Bărbulescu* v *Romania* [GC] App no 61496/08 (ECtHR, 5 September 2017), paras 109 and 111; *López Ribalda and Others* v *Spain* [GC] App no 1874/13 and 8567/13 (ECtHR, 17 October 2019), paras 109–110; *Schüth* v *Germany* App no 1620/03 (ECtHR, 23 September 2010), para 54; *Platini* c *Suisse* Requête no 526/18 (ECtHR, 11 February 2020), para 59.

or a private entity, data protection can be viewed as giving rise to negative or positive obligations on the state respectively.

The wording of Article 8.2 ECHR is explicit about the state's duties not to interfere. In such cases, three questions, deriving from the wording of the Article, should be addressed, namely:

(1) whether the interference was in accordance with the law;
(2) whether the interference pursued the legitimate interests;
(3) whether the interference was necessary in a democratic society.

Conversely, the Convention does not specify the state's positive obligations to ensure the effective realisation of the rights. However, the ECtHR, referring to the purpose of the Convention, has developed an extensive practice on these duties.[24] As opposed to the reasoning of the ECtHR on the duty not to interfere, the assessment of a state's compliance with their obligations to act in a specific situation does not always have a stable or transparent structure.[25] The ECtHR justifies this by stating that the substance of a duty to act under Article 8 may differ depending on the area of private life.[26]

In the employment-related case law on failure to act, the ECtHR usually discusses positive obligations of two types.[27] The first type is the state's duty to install regulations or ensure that a legislative framework is in place to enable the full realisation of the rights.[28] This obligation is related to legality and question 1 of the negative obligations test, although slightly reversed.

The second type of positive obligation is the duty to ensure proportionality of the data usage—which is often referred to as "fair balance" because it relates to the balance between the different interests at stake. The reasoning on "fair balance" is somewhat similar to the reasoning on proportionality regarding negative obligations (questions 2 (legitimate interests) and 3 (necessary-in-a-democratic-society) of the test).[29]

To summarise, although the ECtHR's reasoning in cases concerning the duty to act or not to act may often be very similar, there is a slight difference in the approach to legality requirements. Therefore, in the cases of B and C, depending on whether the employers are

---

[24] *Christine Goodwin* v *the United Kingdom* [GC] App no 28957/95 (ECtHR, 11 July 2002), para 74; *Airey* v *Ireland* App no 6289/73 (ECtHR, 9 October 1979), paras 32–33; *A.* v *the United Kingdom* App no 100/1997/884/1096 (ECtHR, 23 September 1998) para 22; Alastair Mowbray, *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights* (Hart Publishing 2004) 186.

[25] Vladislava Stoyanova, 'The Disjunctive Structure of Positive Rights under the European Convention on Human Rights' (2018) 87(3) Nordic Journal of International Law 344, 346 f.

[26] *Bărbulescu* v *Romania* [GC] App no 61496/08 (ECtHR, 5 September 2017), para 113; *López Ribalda and Others* v *Spain* [GC] App no 1874/13 and 8567/13 (ECtHR, 17 October 2019), para 112.

[27] *Bărbulescu* v *Romania* [GC] App no 61496/08 (ECtHR, 5 September 2017), paras 115 and 120; *López Ribalda and Others* v *Spain* [GC] App no 1874/13 and 8567/13 (ECtHR, 17 October 2019), paras 113 and 116; *Schüth* v *Germany* App no 1620/03 (ECtHR, 23 September 2010), para 57; *Köpke* v *Germany* App no 420/07 (ECtHR, 5 October 2010).

[28] *López Ribalda and Others* v *Spain* [GC] App no 1874/13 and 8567/13 (ECtHR, 17 October 2019), para 110.

[29] *Fernández Martínez* v *Spain* [GC] App no 56030/07 (ECtHR, 12 June 2014), para 114; *Dubská and Krejzová* v *the Czech Republic* [GC] App no 28859/11 and 28473/12 (ECtHR, 15 November 2016), para 165; *Schüth* v *Germany* App no 1620/03 (ECtHR, 23 September 2010), para 55; *cf. Kotov* v *Russia* [GC] App no 54522/00 (ECtHR, 3 April 2012), para 110; Mowbray (n 23) 186 f.

linked to a state or are private companies, the formulation of requirements for compliance might be slightly different.[30]

2.3 REQUIREMENT OF LEGALITY FOR NATIONAL LAW

As explained in section 2.2, the next step of the ECtHR's assessment is to examine the requirement of legality. In those cases that concern negative obligations (where the employer is a state authority or company linked to the state), the requirement of legality means that the interference with privacy must be in accordance with the law. If the case concerns positive obligations (where the employer is a private entity), the ECtHR will analyse if the state has created a legislative framework that safeguards against abuse. In this section, these two reiterations of the requirement for legality are discussed.

The examination of whether an interference was in accordance with the law requires considering the domestic legal system in question. The Convention does not establish any requirements as to the form of domestic law. The requirement is fulfilled, disregarding who regulates the issue—Parliament, the Government, or other actors — as long as this regulator has decision-making powers under national law.[31] The mere existence of national regulations of some sort is considered insufficient, as the law must possess certain qualities, namely, to be foreseeable and accessible.[32] When discussing foreseeability, the ECtHR assesses the availability of practice and guidelines. The absence of, or self-contradicting answers in these sources, can indicate a lack of foreseeability.[33]

In an employment context, the ECtHR deems that absolute precision can be neither expected nor is it desirable: it is not required that the law defines different types of conduct in detail, but the rules can be described in broad terms.[34] The reasoning behind this is that the parties are considered equal in employment relations, as they are based on equal contracts rather than on power relations.[35]

When positive obligations to regulate in an employment context are discussed, the ECtHR, as a rule, reiterates that the states enjoy broad discretion in deciding how to regulate. The national legislator may choose whether the regulation should be embodied in labour, civil, constitutional, administrative, or criminal law.[36] Concerning the obligation to regulate employees' data protection, two requirements of domestic law are repeatedly considered. First, domestic law must ensure that there are sufficient procedural safeguards against abuse.

---

[30] C's disclosure of information based on national regulation means that the state's negative obligations are involved. However, as shown in the previous section, the mere fact that health data is disclosed to the employer will likely not reach a minimum level of severity. The ECtHR will therefore view the case in light of the reason-based approach, evaluating the justification of the employer's decision rather than the fact that the national regulation demands disclosure. See similar reasoning in *Budimir* v *Croatia* App no 44691/14 (ECtHR, 16 December 2021) para 58, where positive (and not negative) obligation became a subject of discussion.

[31] *Wretlund* v *Sweden* App no 46210/99 (ECtHR, 9 March 2004).

[32] *Mateescu* v *Romania* App no 1944/10 (ECtHR, 14 January 2014), para 29; *Peck* v *the United Kingdom* App no 44647/98 (ECtHR, 28 January 2003), para 64; *Y.Y.* v *Russia* App no 40378/06 (ECtHR, 23 February 2016), paras 57–58.

[33] *Oleksandr Volkov* v *Ukraine* App no 21722/11 (ECtHR, 9 January 2013), para 185; *Surikov* v *Ukraine* App no 42788/06 (ECtHR, 26 January 2017), paras 80–81; *Köpke* v *Germany* App no 420/07 (ECtHR, 5 October 2010); *cf. Libert* v *France* App no 588/13 (ECtHR, 22 February 2018), para 44; see also *Antović and Mirković* v *Montenegro* App no 70838/13 (ECtHR, 28 November 2017), paras 59–60.

[34] *Oleksandr Volkov* v *Ukraine* App no 21722/11 (ECtHR, 9 January 2013), paras 176–177.

[35] *Bărbulescu* v *Romania* [GC] App no 61496/08 (ECtHR, 5 September 2017), paras 117–118.

[36] *Bărbulescu* v *Romania* [GC] App no 61496/08 (ECtHR, 5 September 2017), paras 115–116.

Second, it shall see to that any interference with privacy in relations between private parties is proportional.[37] Other than these requirements, the obligation has not been specified.

The broad margin of discretion regarding how to regulate, and the lack of case law on the right to privacy in employment relations, make it difficult to determine whether there are other more specific positive obligations in this field. For the cases of B (bipolar disorder) and C (HIV diagnosis), these requirements mean that if the domestic legal system does not allow any procedural safeguards against unlawful interference into privacy, Article 8 ECHR is likely to be violated. It also means that domestic law must impose the duty on decision-makers to identify conflicting interests that exist, including B and C's interest of privacy, and oblige the decision-makers to make a proportionality assessment. This identification of conflicting interests is also referred to as a "fair balance" test, and its material substance will be discussed further.

2.4 BALANCING EXERCISE

Once the ECtHR is satisfied that the requirements of legality are fulfilled, it assesses the legitimacy of the interests, or put differently, if the purposes for interfering with the employee's right to privacy were permissible. This part of the assessment derives from the language of Article 8.2 ECHR and serves to assess compliance with the duty not to interfere. The examination of legitimate interests is also a consistent part of the "fair balance" test in evaluating the state's duty to act.[38] Article 8.2 ECHR enlists interests that can be regarded as legitimate; these include public safety, protection of health, prevention of disorder and the rights of others. The varying reasons for employers to process information about employees' health may include ensuring workers' or clients'/customers' health and safety, assessing the lawfulness of absence at work, customising rehabilitation schemas, or various communications concerning insurance. They all pursue legitimate interests under Article 8.2 ECHR.[39]

Returning to our cases, in B's situation, the information on his bipolar diagnosis is provided to ensure a safer working environment and psychological support. In the case of C, the information on her HIV diagnosis is used to ensure patient safety. Therefore, neither case B nor C raise concerns about the employers' legitimate interests in processing employee health data (as mentioned above, A's Covid-19 related case does not pass the definitional threshold and, therefore, is not discussed further in the ECHR analysis).

As part of the necessary-in-a-democratic-society test for negative obligations, the ECtHR analyses whether the measures taken by the state are proportional to the legitimate interests and answers to "pressing social needs".[40] The ECtHR will usually start with identifying different interests at stake.[41]

---

[37] *López Ribalda and Others* v *Spain* [GC] App no 1874/13 and 8567/13 (ECtHR, 17 October 2019), paras 112–114; *Bărbulescu* v *Romania* [GC] App no 61496/08 (ECtHR, 5 September 2017), paras 120, 122.
[38] *López Ribalda and Others* v *Spain* [GC] App no 1874/13 and 8567/13 (ECtHR, 17 October 2019), para 134.
[39] See *e.g. Surikov* v *Ukraine* App no 42788/06 (ECtHR, 26 January 2017), para 91.
[40] *Mile Novaković* v *Croatia* App no 73544/14 (ECtHR, 17 December 2020), paras 58–61; *Polyakh and Others* v *Ukraine* App no 58812/15, 53217/16 59099/16 and 23231/18 (ECtHR, 17 October 2019), para 283; *Fernández Martínez* v *Spain* [GC] App no 56030/07 (ECtHR, 12 June 2014), para 124.
[41] *Fernández Martínez* v *Spain* [GC] App no 56030/07 (ECtHR, 12 June 2014), para 123; *Mile Novaković* v *Croatia* App no 73544/14 (ECtHR, 17 December 2020), paras 61–66; *Pişkin* v *Turkey* App no 33399/18 (ECtHR, 15 December 2020), paras 222–227.

For positive obligations under Article 8, the "fair balance" test is used. The test is substantially similar to the necessary-in-a-democratic-society test for negative obligations. This test means that the interests of the employer and employees should be identified and weighed against one another. In case law on positive obligations, the ECtHR explicitly requires that national actors, in their decision-making, recognise the privacy of employees as one of the interests at stake.[42] The ECtHR does not state any other explicit requirements for weighing these interests.

After identifying the interests at stake, the ECtHR turns its attention to the margin of appreciation or the states' discretion in choosing the means to achieve the competing interests. This margin depends on the interests identified. Since the Convention has a subsidiary function, the states are often considered to be in the best position to determine the means necessary for achieving legitimate interests.

The ECtHR often reflects that the protection of health, safety, or prevention of disorders at work falls within a broad margin of appreciation. An example to confirm the broad margin to protect safety can be provided. In *Wretlund* v *Sweden* an employee at a nuclear power plant—an office cleaner—was subjected to compulsory drug tests. Although the employee did not have access to sensitive security areas, the ECtHR considered these examinations as compliant with Article 8, and the case inadmissible. The interest of safety weighed more than the interest of privacy.[43] The broad margin is also clearly visible in data protection case law outside employment relations. In *Y* v *Turkey*, the ECtHR considers that usage of the information about the applicant's HIV status within a hospital is proportional to the purpose of protecting the rights and interests of healthcare professionals and patients.[44] Similar weighing is also visible in case law on freedom of religion in employment. In *Eweida and Others* v *the United Kingdom*, the second applicant was forced to expose a religious symbol due to uniform alternation. Wearing the symbol was regarded as dangerous for patient safety. The employer reallocated the applicant to a non-nursing position to protect health and safety. The ECtHR did not examine in any detail how wearing the religious symbol would jeopardise health and safety in a hospital; it pointed out that hospital management is better placed to provide such assessment.[45]

The broad margin also applies to health and safety in hospitals and is relevant for C's case. This margin is explained by the ECtHR giving particular weight to protecting the rights to life and prohibition of torture and inhumane treatment. Since the interests of protecting lives and health weigh heavier than healthcare professionals' rights, the ECtHR regards that states must have more leeway to protect these vital interests.

The margin of appreciation can be narrowed in cases that concern aspects of realising individual rights. For instance, in cases that affect particularly vulnerable groups that have been discriminated against or stigmatised throughout history—such as persons with HIV or

---

[42] *López Ribalda and Others* v *Spain* [GC] App no 1874/13 and 8567/13 (ECtHR, 17 October 2019), para 122; *Köpke* v *Germany* App no 420/07 (ECtHR, October 2010).
[43] *Wretlund* v *Sweden*, App no 46210/99 (ECtHR, 9 March 2004).
[44] *Y* v *Turkey* App no 648/10 (ECtHR, 17 February 2015).
[45] *Eweida and Others* v *the United Kingdom* App no 48420/10, 59842/10, 51671/10 and 36516/10 (ECtHR, 15 January 2013), paras 20 and 99; *Fernandes de Oliveira* v *Portugal* [GC] App no 78103/14 (ECtHR, 31 January 2019), para 104; *Shchiborshch and Kuzmina* v *Russia* App no 5269/08 (ECtHR, 16 January 2014), para 204.

mental disabilities—the margin of appreciation should be narrower.[46] This reasoning means that the ECtHR shall scrutinise in more detail the reasons for states' weighing the conflicting interests at stake in an unfavourable manner for these vulnerable groups, also determining whether the purpose could be achieved with less intrusive means. In such cases where the ECtHR has concluded a violation of Article 8 in employment relations, some form of discriminatory behaviour of the employer has typically been substantiated (in *Mile Novaković*, connected with protected characteristics of ethnicity; in *Özpınar*, a gender; and in *Polyakh and Others*, political opinion). Such cases are also typically related to very intimate aspects of the employee's private life (in *Bărbulescu*, correspondence of intimate character, in *Schüth*, an extramarital relationship with a woman who was expecting his child).[47]

The states' margin of appreciation will also be narrower when there is a European consensus on the impermissibility of certain rights limitations. Although the term "European consensus" has not been defined by the ECtHR, it can be explained as a trend to have a similar approach in the legislation of the Council of Europe states or when many of them are parties of another treaty that establishes specific rules or principles.[48] In its practice on data protection in employment relations, the ECtHR mostly refers to the International Labour Office Code of Practice on the Protection of Workers' Personal Data, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the GDPR.[49] The universal features of these instruments include requirements of the lawfulness of processing the data, prohibition/limitation of processing the data for other purposes than they were collected, keeping the data up-to-date, and providing procedural guarantees.[50] The ECtHR may refer to the GDPR, or other treaties, as a possible indicator for altering the margin of appreciation; however, as this instrument is applicable only within the certain Member States of the Council of Europe, so the ECtHR is not obliged to do that. Identifying this narrower margin of appreciation usually leads the ECtHR to consider whether states used less intrusive means.[51] Whether the ECtHR will deem that the use of health data in employment relations (for the interests mentioned above) falls within the broader or narrower margin of appreciation is unclear at present due to the scarcity of case practice that explicitly addresses this issue. However, narrowing the margin of appreciation through references to the GDPR may be expected in future case law.

---

[46] *Kiyutin* v *Russia* App no 2700/10 (ECtHR, 10 March 2011), paras 62, 64; *Novruk and Others* v *Russia* App no 31039/11, 48511/11, 76810/12, 14618/13 and 13817/14 (ECtHR, 15 March 2016), paras 98, 100–101; see also *Armonienė* v *Lithuania* App no 36919/02 (ECtHR, 25 November 2008), paras 42–47; *Travaš* v *Croatia* App no 75581/13 (ECtHR, 4 October 2016), para 78; *A.-M.V.* v *Finland* App no 53251/13 (ECtHR, 23 March 2017), para 73; *Cînța* v *Romania* App no 3891/19 (ECtHR, 18 February 2020), para 41.

[47] *Bărbulescu* v *Romania* [GC] App no 61496/08 (ECtHR, 5 September 2017), para 136; *Schüth* v *Germany* App no 1620/03 (ECtHR, 23 September 2010), para 74; *Mile Novaković* v *Croatia* App no 73544/14 (ECtHR, 17 December 2020), paras 64–70; *Özpınar* c *Turquie* requête no 20999/04 (ECtHR, 19 October 2010), paras 76–79; *Polyakh and Others* v *Ukraine* App no 58812/15, 53217/16 59099/16 and 23231/18 (ECtHR, 17 October 2019), paras 292–308 and 321.

[48] See *e.g. Vavřička* and *Others* v *the Czech Republic* [GC] App no 47621/13, 3867/14, 73094/14, 19298/15, 19306/15 and 43883/15 (ECtHR, 8 April 2021), para 273; Kanstantsin Dzehtsiarou, *European Consensus and the Legitimacy of the European Court of Human Rights* (CUP 2015) 11.

[49] *López Ribalda and Others* v *Spain* [GC] App no 1874/13 and 8567/13 (ECtHR, 17 October 2019), paras 60–66; *Surikov* v *Ukraine* App no 42788/06 (ECtHR, 26 January 2017), para 74; *Bărbulescu* v *Romania* [GC] App no 61496/08 (ECtHR, 5 September 2017) paras 38–51, 122.

[50] *Surikov* v *Ukraine* App no 42788/06 (ECtHR, 26 January 2017), para 86.

[51] *López Ribalda and Others* v *Spain* [GC] App no 1874/13 and 8567/13 (ECtHR, 17 October 2019), paras 116 and 128.

To summarise and illustrate the ECtHR's reasoning on balancing, we will return to the cases of B and C. To decide whether the decision to reallocate C due to her HIV diagnosis is proportional, one needs to start with identifying the various interests at stake. On the one hand, these include protecting C's private life and not discriminating against C (a sensitive issue due to the history of HIV stigmatisation). On the other hand, there are interests of the employer to ensure the health and safety of other employees and patients at the hospital. As identified earlier, in the ECtHR's case law, the interests of health and safety are usually considered weighty due to the connection with the right to life and freedom from ill-treatment. The ECtHR will likely conclude that, in this case, the state enjoys a wide margin of appreciation to ensure better protection of these weighty interests. To conduct a further assessment, understanding how C's reallocation ensures a safer work environment or improves patient safety is relevant. This assessment signifies the importance of ascertaining what kind of assignment C fulfilled in paediatric care and whether transmission of HIV was even remotely possible. It can also be relevant to compare the risks in the department where C was reallocated to those risks in paediatric care. However, as mentioned above, due to the weight of the interest of protecting lives and safety in hospitals, the ECtHR will likely find that the state is better suited to decide how to protect these interests and will not consider the reallocation to be disproportional.

In the case of B, information about his bipolar disorder is disseminated to all other employees. In this situation, the ECtHR is expected to assess whether there is a foreseeable legal basis for disclosing that information or protection against abuse for unlawful processing of that data. If such a basis exists, the relevant question is whether the purpose of protection of health or security can be achieved with this dissemination.[52] The answer to this question, in particular, depends on the possibilities for providing help within such settings, how many employees and in what capacity they received this information, the way the disease is manifested, the types of assignments B fulfils, including how vital the interests of others are. The types of assignments that B and others fulfil may indicate vital interests at place and broader margin. If the interests of others are not vital, the ECtHR is likely to consider that the case falls within a narrower margin of appreciation, in particular, because B's mental disorder has historically been stigmatised. The other factor that may indicate a narrower margin of appreciation is a European consensus to limit data processing for a different purpose than was originally obtained for. Thus, B's case is likely to be the most prospective for the applicant in the ECtHR among the three cases if no other vital interests are identified.

3 PROCESSING OF EMPLOYEE HEALTH DATA IN THE GDPR

3.1 DATA PROTECTION AS A FUNDAMENTAL RIGHT AND THE NEXUS OF THE GDPR

From the EU perspective, data protection is a legal concept that extends beyond the GDPR. Article 8 of the Charter of Fundamental Rights of the EU, CFR, recognises data protection as a fundamental right, stating that such data must be processed fairly for specified purposes

[52] *Surikov* v *Ukraine* App no 42788/06 (ECtHR, 26 January 2017), para 93.

and on the basis of consent, or some other legitimate basis laid down by law.[53] In this respect, it is of interest to point out that Article 6(3) of the Treaty on European Union[54] holds the rights of the ECHR as general principles of EU law, and that many of the CFR fundamental rights are modelled after their ECHR counterparts.[55] That this regulatory link to the ECHR extends to the area of data protection is also made clear from that Article 52(3) CFR, which states that rights corresponding to those guaranteed by the ECHR should be the same in meaning and scope (while Union law may provide more extensive protection)—coupled with the fact that Article 8 CFR is based on Article 8 ECHR.[56] And, as Article 53 CFR also holds that nothing in the Charter is to be interpreted as restricting or adversely affecting ECHR rights, the right to respect for private life under the ECHR thus sets a minimum standard for the data protection to be offered by the CFR. This does not mean that the EU is formally bound by the ECHR or the ECtHR's case law (the EU has not accessioned). It does, however, mean that the EU is indirectly bound by the ECHR, as the latter must always be obeyed when restricting fundamental rights in the EU.[57] This necessitates that the CJEU interpret the ECHR and ECtHR case law, in order to make sure that any interpretations of EU law do not violate the ECHR (particularly as this would place the Member States in an invidious position).

The above-mentioned circumstances, of course, stretches into the realm of the GDPR. While the Charter certainly is the instrument that is the closest to being an equivalent to the ECHR within EU law, the GDPR is the instrument that is effectively meant to realise the Article 8 CFR data protection rights in the EU. The GDPR can thus be seen as an implementation of the fundamental right to data protection.[58] This effectively means that the ECHR, by proxy of the CFR, sets the minimum standard for the level of protection that the GDPR has to offer.[59] The CJEU must, therefore, also ensure that any interpretation of the GDPR (as well as the predecending Data Protection Directive[60]) is CFR and ECHR compliant. It is, thus, the GDPR that offers the most detailed account for the level of protection that EU law offers for employee health data.

---

[53] Art 8 CFR gives effect to art 16 of the Treaty on the Functioning of the European Union, 13 December 2007, (TFEU) [2016] OJ C202/1, thus primary EU law, which states that everyone has the right to the protection of personal data concerning them.

[54] Treaty on European Union (TEU) [2008] OJ C115/13.

[55] European Parliament, Council of the European Union, European Commission, Explanations (*) Relating to the Charter of Fundamental Rights (2007/C 303/02) [2007] OJ C 303/17.

[56] See the explanation on art 8, European Parliament, Council of the European Union, European Commission, Explanations (*) Relating to the Charter of Fundamental Rights (2007/C 303/02) [2007] OJ C 303/17.

[57] Tobias Lock, 'The ECJ and the ECtHR: The Future Relationship between the Two European Courts' (2009) 8 The Law & Practice of International Courts and Tribunals 375, 382.

[58] van der Sloot (n 4) 11.

[59] Article 1(2) and Recital 2 GDPR. See also rec 4 GDPR and Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paras 69–72.

[60] 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

3.2 DATA PROTECTION AT WORK? MATERIAL SCOPE AND APPLICATION OF THE GDPR IN AN EMPLOYMENT CONTEXT

In the rest of section 3, we will analyse the protection offered by the GDPR to employees in cases A–C. We will start out by focusing on the basic criteria for applicability and how they apply to our cases. These criteria are that the information must consist of protected "personal data" and be "processed".[61]

Regarding the first criteria, personal data is defined as any information relating to an identified or identifiable natural person.[62] We can state that all types of disclosed information in our cases (diagnosis of specific persons with Covid-19, bipolar disorder or HIV) are at the core of what constitutes personal data. Furthermore, these data include information about physical or mental health and, therefore, are at the core of what constitutes health data, which is recognised as a special category of data subject to a stricter data protection regime.[63]

Regarding the second criteria, the answer to whether the employers (who function as controllers under the GDPR) "process" the health data is also affirmative in all cases A–C. "Processing" encompasses any operation or set of operations performed on personal data or sets of personal data, either by automated means or manually if the data are (or intended to be) contained in a filing system.[64] Although this definition is broad, our cases illustrate some of its delineations.

The disclosure of A's Covid-19 test results likely involves processing because the employer intends to collect information on infection cases amongst employees for organisational or health and safety reasons. If the employer stores this data electronically, it is "processed" as "processing by automated means" effectively relates to all processing via computer technologies. If the data only is stored manually, it is still likely to be "processed". As long as the data is structured according to specific criteria, such as the employees' names or a list of Covid-19 cases within the workplace, it is contained in a "filing system". On the corresponding definition of filing systems in the previous Data Protection Directive 95/46/EC, the Art. 29 WP opinioned that most employment records are likely to fall within this definition.[65]

In B's case, processing similarly occurs when the information on his bipolar diagnosis is collected to certify the permissible sickness absence (whether handled electronically or manually). Had the employer chosen to inform B's colleagues of his diagnosis orally, the GDPR would not apply to that particular use (the data is not contained in a filing system). However, the fact that the employer used e-mail as the medium means that processing took place by automated means. In particular, the e-mailing qualifies as "further processing" of that data, which covers any act of processing following the data collection, whether done for the purposes initially specified or for any additional purposes.[66] As further processing only is allowed under strict conditions in the GDPR, we will return to the implications later.

---

[61] Art 2(1) GDPR. The territorial scope of GDPR, art 3, will not be examined here.
[62] Art 4(1) GDPR. See, also, van der Sloot (n 4) 17.
[63] Art 4(15) and 9 GDPR, rec 35 GDPR. See also Case C-101/01 *Criminal proceedings against Bodil Lindqvist* [2003] EU:C:2003:596, para 50. The specific phrasing used in the article is "data concerning health".
[64] Art 2(1), 4(2) and 4(6) GDPR, rec 15 GDPR.
[65] The Art. 29 WP, *Opinion 8/2001 on the processing of personal data in the employment context* (WP 48 13 September 2001), p. 13; see also Case C-25/17 *Jehovan todistajat* EU:C:2018:551, para 57.
[66] The Art. 29 WP, *Opinion 03/2013 on Purpose Limitation* (WP 203 2 April 2013) 21.

Our last case does not include any information about how C disclosed her HIV status or how the employer later contained that health data. However, as the disclosure was mandated by law, the data will be contained in an electronic or manual filing system, such as a medical or HR file—meaning that the employer processes the data. The employer's later use of this data to inform the decision of C's reallocation does not in itself constitute "processing". This is because the GDPR's applicability is related to each discrete set of processing operations that handle the data. For example, data processing would occur at every instance the medical or HR file was accessed by or transmitted within the workplace or included in any new structured documentation related to the employer's decision to reallocate C. This illustrates that the procedural aspects of how the data is collected and used—rather than the purposes it is used for—are decisive for determining the GDPR's applicability. However, and as we will turn to next, what purposes the data is processed for will affect whether the processing is lawful.

3.3 BASES FOR LAWFUL PROCESSING OF EMPLOYEE PERSONAL AND HEALTH DATA

Unlike the ECHR, the GDPR formally recognises the specificity of data processing in the context of employment by including some employment-specific provisions.[67] This does not mean that employers are subject to a special data protection regime, as they can still base their processing of employee personal and health data on many of the non-employment-specific provisions of the GDPR. As we will see, however, the employment-specific provisions make GDPR more adaptable to Member States and labour market conditions when concerning employee data protection.

The basic conditions for processing any personal data are laid down in Article 5 GDPR. Of these, the principles of lawfulness, purpose limitation (requiring that the purposes for collecting data should be specified and legitimate, as well as restrict the possible further use of that data), and data minimisation (requiring that any data collected are held to a minimum as necessitated by the stated purposes for their use), are particularly relevant for delineating the possible scope of the employer's data processing in cases A–C. These three principles will be our focus, where initial and main attention will be given to the lawfulness criterion.

As introduced, all our cases concern health data, which qualifies as special category data in the GDPR.[68] To lawfully process employee health data, the employer must, therefore, not only show that at least one of the general lawful bases for processing personal data in Article 6 is met. The employer must also demonstrate that the processing is allowed under Article 9, as the article prohibits any processing of special category data unless a derogation applies.[69] In sections 3.3-3.4, we will structure our reasoning by thematically coupling the

[67] See Céline Brassart Olsen, 'To Track or not to Track? Employees' Data Privacy in the Age of Corporate Wellness, Mobile Health, and GDPR' (2020) 10 International Data Privacy Law 236, 242; Maja Brkan, 'Introduction: Employee's Privacy at the Forefront of Privacy Debates' 3 European Data Protection Law Review (Internet) 543, 543–544.

[68] Art 9 GDPR.

[69] The legal basis/bases in each of the articles need not be linked, Rec 51 GDPR and Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, *Minutes of the Second Meeting* (2016) 2.

different bases of both articles, as either allowing for processing to cater to employer needs or to public interest needs.

3.4 LAWFUL PROCESSING FOR EMPLOYERS TO CATER TO THEIR OWN NEEDS

This section focuses on the conditions allowing employers to lawfully process health data to cater to their own obligations or interests.

First off, the processing of personal data may be allowed if the employer has asked for the employee's consent, Article 6(1)(a) GDPR. However, it is questionable whether consent may offer a legal basis for processing employee health data.[70] Article 4(11) GDPR defines consent as being freely given, specific, informed, and unambiguous. The related Recital 42 states that "freely given" implies a genuinely free choice for the data subject to be able to refuse or withdraw consent without detriment.[71] Specifically, Recital 43 also states that consent should not provide a valid legal basis for processing where there is a clear imbalance between the data subject and the controller. The Art. 29 WP has reasonably argued that employer-employee relations are of clear imbalance due to the latter's financial dependence on the former. It has been suggested that consent is "highly unlikely" as a legal basis for data processing at work unless employees can refuse without adverse consequences.[72] At the same time, Recital 155, adding specificity to Article 88 GDPR, states that Member State laws or collective agreements may regulate the conditions under which processing may be based on employees' consent. Altogether, this suggests that consent in an employment context may be a sufficient basis for the lawful processing of personal data, but that the employer-employee interests balancing should be done by a legislator or via collective bargaining—and not on an individual basis.

If no adverse consequences are linked to incompliance—as in A's case—the choice to comply with a policy to disclose Covid-19 tests results might meet the conditions for consent under 6(1)(a). However, as the case concerns health data, the consent must meet the additional requirements in Article 9(2)(a) GDPR—that it needs to be explicit, not implied. This means that a high degree of consent precision and definiteness, including a specific description of the purposes of the processing is required.[73] The GDPR emphasis on freely given consent suggests that the assessment should not be limited to formal or pre-stated sanctions. Instead, the assessment shall be contextual and encompass all factors that can affect the employees' position when asked or encouraged to consent. The mere absence of sanctions for incompliance in a workplace policy does not suffice to ensure that the employee is in a position to consent freely in the meaning of Article 9(2)(a) GDPR.

---

[70] Art 7 GDPR sets out a number of conditions for consent, which will not be elaborated here.

[71] That consent should be given "freely" is in alignment with the principle of fairness in art 5(1)(a) GDPR. 41, Lee A Bygrave, 'Core Principles of Data Privacy Law' in Lee A Bygrave (ed), *Data Privacy Law: An International Perspective* (OUP 2014) 146 f. See also Case C-673/17 *Planet 49* EU:C:2019:801, para 52, on that consent points to active rather than passive behaviour from the data subject.

[72] The Art. 29 WP, *Opinion 2/2017 on data processing at work* (WP 249 8 June 2017) 3; The Art. 29 WP, *Opinion 03/2013* (n 66) 3. The Council of Europe and the European Union Agency for Fundamental Rights have also jointly made similar conclusions. European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law: 2018 edition* (Publications Office 2018) 144.

[73] Ludmila Georgieva and Cristopher Kuner, 'Article 9 Processing of Special Categories of Personal Data', in Lee A Bygrave, Cristopher Docksey and Cristopher Kuner (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP Oxford 2020) 377.

For assessing if consent is freely given, the specific type of health data the case concerns must also be considered, including the level of sensitivity and stigma attached. However, the permissibility of consent as a basis for processing data in an employment context is still not clear in all respects. Suder shows that Member State Data Protection Authorities (DPAs) express different opinions in their guidelines on consent to process personal data in workplaces.[74] Further clarifications on the scope of Articles 6(1)(a) and 9(2)(a) in an employment context in future CJEU case law would therefore be welcome.[75]

Therefore, consent may be a problematic basis for the routine processing of employee (personal and) health data. The generally most important legal basis for processing employee personal data is Article 6(1)(f), allowing processing necessary for the legitimate interests pursued by the controller.[76] Any such processing must be strictly necessary for a legitimate purpose, which must outweigh the employees' privacy rights in the workplace.[77] Recital 48 indicates that the employer's legitimate interests include transmitting employee personal data for internal administrative purposes. However, there is no basis in Article 9 that permits processing of special category data under a general balancing of interests. So even if a safer working environment and psychological support could qualify as legitimate interests to the employer, they would not by themselves enable the internal communication on B's bipolar disorder within the workplace. The same is true for any potential further processing of nurse C's HIV diagnosis related to the administration of her reallocation.

Of greater relevance for processing health data in workplaces are Articles 6(1)(c) and 9(2)(b) GDPR. Article 6(1)(c) allows data processing when necessary for compliance with legal obligations to which the controller (employer) is subject. Article 9(2)(b) does not directly correspond to 6(1)(c) but is of interest for finding the additional basis required to process sensitive data. The article expressly enables the processing of health data necessary to carry out the obligations and exercise specific rights of the controller or the data subject for employment, social security, and social protection. Article 9(2)(b) is also dependent on special regulation: the processing must be authorised by Union or Member State law or a collective agreement under Member State law. Such obligations must not include a specific law for each individual processing. A specific regulated obligation could therefore enable different kinds of processing activities. However, each processing must be necessary to fulfil obligations or exercise the rights of employers or employees.[78] Notably, Article 9(2)(b) applies to the rights and obligations of employers and employees. Depending on the specific rights or obligations, such as employee rights to lawful sick leave or employer obligations to provide for a safe

[74] Seili Suder, 'Processing Employees' Personal Data during the Covid-19 Pandemic', (2020) 12 (3) European Labour Law Journal (Internet) 1, 9. Suder's analysis was primarily based on Covid-19 related guidance issued by 20 DPAs of the Member States. See also Mahsa Shabani, Tom Goffin and Heidi Mertes, 'Reporting, recording, and communication of COVID-19 cases in workplace: data protection as a moving target' (2020) 7 (1) Journal of Law and the Biosciences.

[75] Art 9(2)(e) GDPR allows processing when sensitive data (such as health data) has been manifestly made public by the data subject. This basis bears some kinship to consent, but is not relevant to the cases A–C and will not be explored in this article.

[76] This basis does not apply to processing carried out by public authorities in the performance of their tasks, art 6(1) GDPR.

[77] The Art. 29 WP, *Opinion 2/2017* (n 72) 23. See also, Claudia Oriseg, 'GDPR and Personal Data Protection in the Employment Context' (2017) 3 Labour & Law Issues 1, 12.

[78] Rec 45 GDPR. See, also, rec 41 GDPR.

working environment, Article 9(2)(b) may therefore unlock employers' possibilities to process data in many situations.

Returning to our cases, a regulation placing such obligations on employers that necessitates testing or reporting of Covid-19 cases amongst employees could enable processing in case A. The obligation must not specify the collection of Covid-19 test results, but could relate to health and safety at work or obligations justified by public interests that are specifically directed at the employer. In the case of B, social security or employment regulations creating obligations related to employee sickness absence could enable processing. Employer C is subject to national patient safety regulations obliging her to disclose her HIV-positive status. However, as will be elucidated later, Member State regulations must also be based on legitimate purposes and only allow personal data processing necessary to achieve those purposes.

Furthermore, Article 9(2)(h) GDPR can also be relevant for discussion. It allows for processing health data when required for preventive or occupational medicine, assessing the employee's working capacity, or managing health or social care systems and services. However, it only allows processing by, or under the responsibility of, a professional subject to the obligation of professional secrecy.[79] The provision, for example, enables health care professionals to help the employer assess work performance. It does not enable employers to process the data themselves, and would therefore not enable processing in the cases A–C.

As seen, employers can rarely rely on consent for processing employee health data. The most viable ground for employers to process such data is, therefore, when necessitated by the fulfilment of obligations or ensuring of employee rights, as allowed by Article 9(2)(b) GDPR. Notably, for the employment context, such rights and obligations could also be laid down in collective agreements (if pursuant to Member State law).

3.5 LAWFUL PROCESSING FOR EMPLOYERS TO CATER TO PUBLIC INTERESTS

This section focuses on the GDPR's possible legal bases for employers to lawfully process health data to cater to other (external) needs than their own, and primarily those of public interest.

Starting with Article 6(1)(e) GDPR, it permits processing if necessary for performing tasks of public interest, based on Union or Member State law. Correspondingly, Article 9(2)(g) GDPR allows the processing of sensitive data if the regulated public interest qualifies as "substantial". Recital 45 clarifies that the healthcare sector—employer in case C—is of public interest. However, the specific patient safety risk posed by C's HIV diagnosis is unlikely to qualify as "substantial" in this regard. This is indicated by Recital 46, which provides no definition of "substantial" interests, but exemplifies the less sharply worded "important grounds" of public interest as processing necessary for monitoring epidemics and their spread or in situations of humanitarian emergencies. These examples indicate that the public interests should be of a larger scale than in case C. The EDPB has in its Covid-19 specific statement, referred to substantial public interests as a plausible option for employers

[79] Art 9(3) GDPR.

to process health data to control health threats, as relevant to case A.[80] The dependence on Union or Member State law, however, underlines that more specific regulation must set out the purposes and grounds that reflect a substantial public interest.[81] Notably, this basis would therefore be relevant in cases where the public interests are laid out in law but not specifically addressed to employers in the form of legal obligations (for which case the Articles 6(1)(c) and 9(2)(b) would be more viable).

Lawful processing could also take place if necessary to protect the vital interest of the data subject or another natural person under Article 6(1)(d). Recital 112 indicates that "vital interests" include the physical integrity or life of the person. When the data are sensitive, such as health data, the corresponding basis in Article 9.2(c), however, only allows for processing when the data subject is physically or legally incapable of giving consent. Therefore, the significance of Article 6(1)(d) in an employment context and its relevance for our cases A–C is limited. The EDPB has mentioned this basis as lawful for employers to process special category data, such as health data, in emergencies.[82]

Finishing off with Article 9(2)(i) GDPR, it has no directly corresponding basis in Article 6, but enables processing necessary for reasons of public interest in the area of public health based on Union or Member State law (such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare). This basis is, therefore, particularly relevant for case A, and the EDPB (in its Covid-19 statement) foresaw its possible use to employers in processing health data when taking the already introduced Recital 46 into consideration.[83] However, Recital 54 clarifies that such processing should not result in personal data being processed for other purposes by third parties such as employers. Insofar as Article 9(2)(i) may be applicable in an employment context at all, it may therefore never be used to serve employer needs. It is rather intended for use by public health authorities, non-governmental organisations and other entities working in areas such as disaster relief and humanitarian aid.[84] However, some Member State DPA's consider that employers can rely on this basis to process employee health data relating to Covid-19 when executing explicit instructions and acting on the advice of competent authorities.[85]

To summarise, the most plausible bases for unlocking processing capabilities for employee health data in relation to our cases are Article 9(2)(g) GDPR, substantial public interests, and Article 9(2)(i), processing necessary for reasons of public interest in the area of public health. Both of these bases might be relevant, in particular, to case A. They also share that they have been made dependent on further EU or Member state regulation, which clarifies that "public interests" should be laid out in law.

3.6 PROCESSING PROVIDED FOR BY SPECIFIC REGULATION

Our observations in previous sections indicate that the GDPR allows the processing of employee health data in many—although specific—situations. As shown, consent is not a

[80] EDPB, *Statement on the processing of personal data in the context of the COVID-19 outbreak* (EDPB, 19 March 2020) 1 f.
[81] See, also, rec 52 GDPR.
[82] See EDPB (n 80) 2.
[83] EDPB (n 80) 2.
[84] Georgieva and Kuner (n 73) 380.
[85] Suder (n 74) 8.

particularly viable ground while not entirely precluded. Furthermore, most of the examined legal bases in Article 6 and all the examined derogations in Article 9, have been made dependent on specific regulations. This reliance on specific regulation allows the Member States to take divergent regulatory approaches and de facto create different protection levels of employee health data between states.[86] However, it is also clear that the Member State's mandates to install such provisions are subject to limitations.

Especially important as a restricting factor to the Member State's space for regulatory manoeuvre is the already introduced aspect that any national rules, even when installed under the approval of the GDPR, will be subordinate to (and evaluated against) the basic standards of data protection set by the CFR and ECHR. The CFR, as well as the ECHR, are therefore integral benchmarks for the right to data protection in the GDPR. One important manifestation of this permeation of human and fundamental rights into the GDPR, is the established CJEU case law that the Member States' derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (which includes that the measures adopted must be less intrusive compared to other options for achieving the same goal).[87] The necessity of the legislation must, in particular, also be evaluated against the Member States' stated reasons for that specific regulation. Referencing Article 52(1) CFR, the CJEU has, for example, dismissed national legislation providing for public access to personal data because such unrestricted access was not necessary to achieve the stated objective of improved traffic safety.[88] This implies a requirement for the Member States to clarify the objectives of any specific regulation they install.

The GDPR's anchoring in fundamental rights is also underlined by the fact that the Member States' space for regulatory manoeuvre often is restricted by obligations to combine the specific regulation with safeguards aimed at protecting the rights of the data subjects. This is the case for any Union or Member state regulation allowing the processing of special category data, such as health data.[89] It is also the case for any employment specific regulation or collective agreements installed under Article 88(1) GDPR.[90] Such rules could include specific rules regarding data processing for the discharge of obligations, health and safety at work, and the enjoyment of rights and benefits related to employment— but must include safeguards aimed at protecting the employee's human dignity, legitimate interests, and fundamental rights. Particular regard should also be given 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 workplace.[91] This

---

[86] Rec 10 GDPR.

[87] See case C-13/*16 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme* EU:C:2017:336, para 30, and cited case law.

[88] Case C-439/19 *B v Latvijas Republikas Saeima* EU:C:2021:504, paras 105, 115–122.

[89] Article 9(4) and rec 52 GDPR. See also, for example, Article 23(1); Emanuele Ventrella, 'Privacy in emergency circumstances: data protection and the COVID-19 pandemic' (2020) 21 ERA Forum 379.

[90] Patrick Van Ecke & Anrijs Šimkus, 'Article 88 Processing in the Context of Employment' in Lee A. Bygrave, Christopher Docksey and Christopher Kuner (eds), *The EU General Data Protection Regulation (GDPR): A commentary* (OUP 2020) 1234, 1237.

[91] Article 88(2) GDPR. See also rec 155 GDPR; Paul De Hert and Hans Lammerant, 'Protection of personal data in work-related relations', Study made on behalf of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (*Publications Office* 2013) 67. Currently pending before the CJEU is a request for a preliminary ruling on whether national rules not meeting these safeguarding-requirements nevertheless can remain applicable, case C-34/21 Hauptpersonalrat der Lehrerinnen und Lehrer beim

indicates that prioritised safeguarding measures are those aimed at restricting the free flow of employee data within large and complex employer organisations, as well as those that help make employees aware of occurring processing activities (to enable better watching over that data protection rights are respected).

As put by Wagner and Benecke, the utilisation of GDPR opening clauses by Member states leads to a complex system of legal provisions requiring the addressees of those provisions, such as employers, to have a deep understanding of the relationship between European and national law.[92] This conclusion also extends to the requirements of having appropriate safeguards in place, where the specific content and effectiveness of privacy-protecting measures also need to be considered in a multi-layered legal structure. This shows that the GDPR seldom operates in isolation (as a stand-alone regulation) in the context of employment.

3.7 PURPOSE LIMITATION AND DATA MINIMISATION

We will now return to the principles of purpose limitation and data minimisation and their possible effects on our cases. Because, even if a lawful basis for processing employee health data has been established in accordance with Articles 6 and 9 GDPR, and even if there was specific regulation in place to support that particular processing, these principles are key to preventing excessive use of the data.

The purpose limitation principle holds that data must be collected for specified, explicit, and legitimate purposes (purpose specification) — and that it may not be further processed in a manner incompatible with those purposes (compatible use).[93] While A's case does not involve any apparent further processing of the collected data, B's case does. The employer's stated reasons, to provide a safe working environment and psychological support for B, are clearly different from certifying B's permissible sick leave. Therefore, further processing in B is only lawful if it passes the compatible use test. In this test, consideration should be given to factors such as the links between the original purpose and the upcoming purpose, and the contexts where the data has been collected (where the relationship between the data subject and the controller is relevant). Similarly, the data sensitivity, including the possible consequences of the intended further processing, and the existence of appropriate safeguards, shall be regarded.[94] The Art. 29 WP has expressed that the more sensitive nature of the data involved, the narrower the scope for compatible use (which is in line with the express requirement in Article 6(4) to consider the nature of the data).[95]

Here, B's subordinate position to his employer, combined with the fact that the bipolar disease is sensitive information, indicates a narrow scope and that the further processing

Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums, Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany), lodged on 20 January 2021.

[92] Julian Wagner & Alexander Benecke, 'National Legislation within the Framework of the GDPR' (2016) 2 European data protection law review 353–361.

[93] Art 5(1)(b), 6(1)(b) and rec 39 GDPR. Art. 29 WP, *Opinion 03/2013* (n 66) 11 f.; Cécile de Terwangne, 'Article 5. Principles relating to processing of personal data' in Lee A. Bygrave, Cristopher Docksey and Cristopher Kuner, *The EU General Data Protection Regulation (GDPR): A commentary* (OUP Oxford 2020) 315.

[94] Article 6(4) GDPR. See also, rec 50 GDPR.

[95] Art. 29 WP, *Opinion 03/2013* (n 66) 25.

would not pass the compatible use test. Informing B's colleagues without either B's consent or a basis in Union or Member State law would, therefore, be unlawful.

In C's case, we do not know whether any further processing occurred, although it is likely that C's HR or medical file was accessed or transmitted within the workplace during her reallocating to another department. Any such further processing would most probably be covered by the original purpose set by the obligating regulation—to protect patient safety (by reducing the risk of infectious disease spreading). Therefore, the circumstances of case C do not indicate that the purpose limitation principle would pose a limitation.

Moving on to the data minimisation principle, it holds that any processing should be adequate, relevant, and limited to what is necessary for the purposes of the processing.[96] This marks that the necessity and proportionality must be assessed for each specific processing rather than be based on general considerations.[97]

In our cases, the fact that employee A is working from home may call the necessity of processing Covid-19 test results into question. However, the conclusion is dependent on the specific purpose of the processing. Especially if the employer's processing is aimed at complying with a directly regulated obligation, it is likely to suffice as necessary. Where the purposes for processing are only indirectly linked to the employer, such as when prompted by public interests (like preventing the spread of a virus), the necessity of the particular processing must be assessed in relation to the employer's role in aiding those purposes. This limits the employer's conditions to take on tasks on its own initiative to serve public interests.

B disclosed his bipolar disorder diagnosis to certify his sickness absence. This fact will likely meet the necessity requirement for processing as long as the information is needed for the employer to be able to assess B's incapacity to work.

For C, even if there is a legal obligation to disclose health-related information for patient safety reasons, the necessity of the employer's processing will be assessed in relation to what type of data is covered by the disclosure obligation. If the obligation is not explicitly directed at infectious diseases or HIV status, but relates to more abstract criteria, such as the risk of endangering patient safety, the necessity of the processing must be assessed. In this assessment, C's function and specific work tasks are relevant.[98]

According to CJEU data protection case law, only those measures limiting the right to data protection that have proved to be necessary should proceed to the next step, the proportionality test.[99] Here, the proportionality assessment will have to be made for each specific processing and aim to identify whether the advantages of the measure outweigh the

---

[96] This corresponds to the requirement of art 52(1) CFR which states that any limitation on the exercise of the right to personal data protection, art 8, must be "necessary" for an objective of general interest or to protect the rights and freedoms of others.

[97] See also rec 4 and 39. On the link between the data minimisation principle and proportionality, see also case C-708/18 *TK v Asociația de Proprietari bloc M5A-ScaraA* EU:C:2019:1064, para 48.

[98] Jana Žuľová, Marek Švec and Adam Madleňák, 'Personality Aspects of the Employee and their Exploration from the GDPR Perspective' (2018) 1 Central European Journal of Labour Law and Personnel Management 68, 74.

[99] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* EU:C:2010:662, paras 86–89; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238, paras 92–98; case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650, paras 92–93; European Data Protection Supervisor, *Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (EDPS, 11 April 2017) 5.

disadvantages it causes concerning fundamental rights.[100] As the proportionality must be assessed before the processing is carried out, the assessment cannot be based on the actual consequences that the specific data processing had for either employee A, B, or C. The assessment shall be based on the stated purpose and known circumstances at the time of processing and relate to the abstract and general risks that the processing could render.

The employer is thus obliged to justify each instance of processing personal data with a specific purpose and assess its necessity and proportionality to keep the processing to a minimum.[101] The GDPR thus prescribes as well as premises that employers have an active and conscious approach to all employee data processing within the workplace.

4 COMPARING THE INSTRUMENTS

It is now time to outline our conclusions. We will do this by comparing the level of protection for employee health data offered by the ECHR and GDPR. To highlight the identified differences in the interpretive steps for assessing the permissibility of using or processing such data, we will return to the fictive cases suggested at the beginning of this article.

In the first case, A disclosed positive Covid-19 test results to comply with an internal workplace policy. Our study indicates that cases similar to A's are unlikely to render the ECHR applicable. To invoke the right to privacy in employment relations, one must show a significant impact on private life or that there are employment-related consequences for the employee. In our example, neither the impact reaches the minimum level of severity nor has the employer made an employment-related decision due to A's disease. The structure of Article 8 ECHR means that whether consent to disclosure was given voluntarily is of no importance, the impact on the private life of the individual is in focus. Here, the fact that the health data disclosure was without prescribed consequences for incompliance has a significant bearing on this conclusion. The threshold for application of Article 8 ECHR has not yet been reached in the case of A.

When A's case is assessed from the GDPR's perspective, the more static nature of the scope of protection becomes evident. The applicability is not dependent on the actual consequences for A. Whether "processing" of protected data has occurred is assessed independently of A's particular private life impact. As the GDPR displays a hesitant position on whether consent really can be "freely" given in the employment context, the voluntariness of A's disclosure can be questioned even if there are no stated sanctions. The most viable bases for lawful processing are instead related to the employers' fulfilment of obligations or the ensuring of employee rights, substantial public interests, or public interests in the area of public health—which are all dependent on the existence of specific EU or national regulation (including collective agreements if they place obligations directly on employers). Although our case A omits information on whether any specific regulation was present, our analysis shows that there is no threshold for applicability in the GDPR other than that personal data must be processed. The analysis also shows that employers tasked with serving public

---

[100] Art 52(1) CFR, European Data Protection Supervisor, *Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (EDPS, 11 April 2017) 5.

[101] Article 23(1) GDPR, Dariusz Kloza and Laura Drechsler, 'Proportionality has Come to the GDPR', (*The European Law Blog*, 9 December 2020) <https://europeanlawblog.eu/2020/12/09/proportionality-has-come-to-the-gdpr/> accessed 1 September 2021.

interests (such as curbing the spread of Covid-19) may enjoy a more generous data protection regime in relation to processing employee health data.

The comparison in the case of A allows us to illustrate a substantial difference in reasoning between the ECHR and GDPR on the protection of employee health data. In the ECHR, what health data of the employee that will enjoy protection is determined on the basis of a relational assessment. However, the GDPR offers a static and broad definition of personal data. The notion of personal data in the GDPR, in contrast to privacy interference in the ECHR, is not context-dependent.

We now turn to the case of B, which involved the collection of health data on the employee's bipolar disorder and subsequent disclosure to other employees. The ECHR assessment here will primarily concern the disclosure of health data to others since this act, rather than the collection of data on its own, can significantly affect the employee's private life. Here, the ECtHR would use the consequence-based approach to determine the ECHR's applicability. This approach means that the ECtHR will assess whether the consequences of data disclosure have reached the minimum level of severity for B's private life. Whether an interference has occurred is a subject of dynamic interpretation and dependent on multiple factors, such as the attitude towards disease in a society or persons carrying it or other specific circumstances. We have argued that B's situation likely reaches the minimum level of severity as it has resulted in the inability to maintain social contacts at work.

At the justification stage, the assessment of B's case will concern the legality and proportionality of the interference. As to the legality, the ECtHR considers that the parties—the employer and the employee—are equal in employment relations. The acknowledgement of equal status rather than power relations results in the ECtHR's undetailed acceptance of the legal basis in domestic law. As to proportionality assessment, sharing information with other employees is likely to be considered a too invasive measure. For a qualified judgment, identifying and weighing the interests at stake in a specific case is necessary. Suppose other vital interests of the employer cannot be identified. In that case, B's mental disorder—a condition that historically has been stigmatised—is a factor requiring weighty reasons for sharing the data. If no vital interests of the employer for sharing the data are identified, the state's discretion in choosing whether to interfere with privacy is narrower. In such a case, the ECtHR is likely to find that sharing the data was not a proportionate means to fulfil a legitimate aim and that a violation of Article 8 took place. Furthermore, the ECtHR is likely to consider that the state's powers to decide are restricted due to the European consensus to limit data processing in relation to purposes other than that which the data was obtained for. To identify this narrower margin of appreciation, the ECtHR may refer to the GDPR's purpose limitation principle.

The GDPR reasoning regarding the scope of protection in B's case is similar to A's: the processing is viewed as a static and objective act, where the applicability is assessed independently of the particular consequences of the data that is processed. However, the case involves different instances of processing, which should be assessed separately: the collection of data about B's disease and the dissemination of that same data to others. Regarding the first processing, the regulation forming the basis of the employer's rights or obligations in this regard must, firstly, be proportionate by the standards of the CFR and the ECHR. This is a responsibility that rests with the national legislator. Since the capacity to assess permissible sick leave is an important but not solely unilateral interest of the

employer—but interest also relevant from the employee- as well as ultimately the public perspectives—we argue that specific regulation enabling employers to process such data is likely to be considered proportionate.[102] However, even if the specific regulation installed in accordance with a GDPR opening clause is proportional, this does not by default imply the necessity of processing any data covered by that regulation in the specific case. Employer B must also assess the proportionality of the particular processing following the "necessity-requirements" under Articles 6 and 9 and the data minimisation principle. Thus, employers can not solely rely on the national legislator's abstract proportionality assessment as manifested through regulation, but must also make their assessment before each specific processing—where the specific needs and specific risks the data processing entails for the employee are balanced against each other in more detail. In case B, the employer would have to consider what level of detail would be needed regarding B's condition to assess whether his absence was permissible, and keep the processing to a minimum.

Moving on to the second processing in case B, the purpose limitation principle must be considered. This is due to the data being collected for one purpose and disseminated for another (disclosing information to colleagues). As seen, the more sensitive the information involved, the narrower the scope for compatible use would be. The particular type of data concerned may therefore affect whether further processing is lawful under the original purpose, where information about B's bipolar disorder is particularly sensitive. We, therefore, argue that the second purpose for processing is unlikely to be compatible with the first. The conclusion is that further processing would require either B's consent or a separate basis in law.

For B, the outcome is similar in the ECHR and GDPR. However, this conclusion is reached through assessments focusing on slightly different aspects of the factual circumstances. As Article 8 ECHR is concerned with protecting the private life of persons (rather than just data protection), it approaches the question of permissibility rather broadly by focusing on the impact that the use of the data has on life and relations of the victim. By contrast, the fact that the assessment of lawful processing in the GDPR needs to be made before the event, means that the actual consequences that followed a given act of processing are not relevant regarding its legality,[103] while they may be essential to determine whether there has been an interference with privacy under the ECHR. This is because the GDPR determines the conditions under which the *act* of processing is lawful at the time it is carried out. The GDPR does not, and does not aim to, set out the full conditions for employees' (or other data subjects') right to privacy. As seen, it does not regulate whether employers may require their employees to disclose particular data but whether they are allowed to "process" that same data. The method by which the data is handled is decisive. So, although the GDPR more actively permeates the employer's everyday dealings with employee personal data in workplaces—by regulating every instance of processing—it also displays blind spots that

[102] See, for example, Case F-130/07 *Fiorella Vinci v European Central Bank* EU:F:2009:114, paras 122, 139. In the case, the Civil Service Tribunal did not find excessive, an EU body's collection of health data through the full examination of a staff members' general state of health in order to assess whether repeated sickness absence had been justified. The relevant regulation was the Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[103] The specific consequences may, however, affect the data subject's compensation in case of violation, art 82 GDPR.

employers can utilise. By choosing to inform B's colleagues orally rather than via e-mail, the employer could have avoided GDPR applicability regarding the choice to inform B's colleagues, whilst this detail would not have had any decisive relevance under the ECHR.

The comparison in cases A and B also shows that the ECHR and GDPR recognise the relationship between employers and employees differently. The ECHR predominantly views the parties in employment relations as equals; the power imbalance in employer-employee relations is rarely acknowledged. The employment contract thus justifies a certain interference with privacy by employers under the ECHR. Instead, the GDPR explicitly recognises a general power imbalance between employees and employers in its data protection design, as particularly manifested through the restrictive view on consent. Even though there are several possible grounds in the GDPR that allow employers to process health data within the workplace, the instrument directs the primary focus away from the individual autonomy of the employee. The focus shifts towards the Member States' responsibility to determine, and manifest via the installation of national regulation, what type of data processing employers should be allowed to carry through.

Finally, C's case—a nurse reallocated to another department in the hospital due to her HIV—is likely to render the ECHR applicable. As the employer has made disadvantageous employment-related decisions based on personal life circumstances (namely, having a specific disease), the ECtHR would assess this situation using the reason-based approach and conclude that Article 8 is applicable. However, the ECtHR's broadly permissible approach to proportionality in cases on protection of health would make a violation unlikely. Unless the employee's interests significantly outweigh the employer's interests, states are presumed to have a broad margin of discretion in choosing means. In cases similar to C's, the protection of health and safety usually outweighs employees' interests, and such interference is usually seen as necessary.

The data collection regarding C's diagnosis amounts to "processing" under the GDPR, and is likely to be lawful when necessitated by applicable health and safety regulations. However, the use of C's health data to inform the decision to reallocate her will only be "caught" by the GDPR if the data is "further processed". The broad definition of processing, which includes any access to or transmissions of C's HR or medical files within the workplace, renders some form of further processing of her health data for reallocation purposes likely. In such a case, the further processing would likely be covered by the original purpose set by the obligating regulation—to protect patient safety (by reducing the risk of infectious disease spreading). Under the GDPR, processing occurs here and now, and only circumstances known at the time of processing are relevant to assess the lawfulness. Therefore, whatever impact the processing had on the employee's private life will not directly affect the assessment of whether it was lawful when it was carried out. This means that the compatibility assessment will be independent of whether, for example, the final decision to reallocate C is lawful.

As we see, the ECHR and GDPR also generate similar conclusions for the case of C, that the data usage is likely to be permissible (although derived through different assessments). A circumstance of particular interest in case C is, however, that we know that the disclosure was explicitly mandated by law. We have argued that this type of regulation would most probably suffice to the legality, necessity, and proportionality requirements under both the ECHR and the GDPR due to the type of disease and the purpose of

protecting health, safety, and preventing disorders at work. As the ECHR (by proxy of the CFR) functions as one standard setting instrument for the level of protection that the GDPR has to offer, the case law of the ECtHR under Article 8 ECHR is relevant, although not necessarily conclusive, when assessing whether a limitation is compliant with the CFR.[104] The CJEU's established general condition that any regulation interfering with CFR rights must be "strictly" necessary, indicates a more restrictive view on necessity than indicated by the ECtHR in its employment specific case law (where the court's view of the effect of the employment contract on the balance of power between employee and employer has justified a broad margin of appreciation). So, although it is likely that the mandatory disclosure regulation in case C would pass the bar in both the ECHR and the GDPR, the standards that such regulation needs to meet might be particularly divergent in the employment context. As we have argued, a narrowing of the ECHR margin of appreciation through references to the GDPR might be expected in future ECtHR case law.

To summarise, we have observed that the ECHR and GDPR deliver similar but not identical answers to whether the data usages in cases A-C are permissible. This demonstrates that the instruments offer different levels of protection for employee health data. They do this partly because the instruments showcase different views on the power-balance between employers and employees, and, thus, do not fully overlap with regards to the types of data protected in the context of employment. As illustrated through our examples, they also do it partly because their different legal designs bring the assessments of lawful use or processing into slightly different focuses. Giving thought to these differences is relevant to determining what "the law is" and understanding the interconnectivity of European data protection.

[104] European Data Protection Supervisor, *Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (EDPS, 11 April 2017) 6; Herke Kranenborg, 'Art 8 – Protection of Personal Data' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), *The EU Charter Of Fundamental Rights: A Commentary* (Uppl. 2, Hart Publishing 2014); Case C-601/15 *J.N. v Staatssecretaris van Veiligheid en Justitie* EU:C:2016:84, para 77.

LIST OF REFERENCES

Atkinson J, 'Workplace Monitoring and the Right to Private Life at Work' (2018) 81 (4) The Modern Law Review 688
DOI: https://doi.org/10.1111/1468-2230.12357

Brassart Olsen C, 'To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR' (2020) 10 International data privacy law 236
DOI: https://doi.org/10.1093/idpl/ipaa004

Brkan M, 'Introduction: Employee's Privacy at the Forefront of Privacy Debates' (2017) 3 European data protection law review 543
DOI: https://doi.org/10.21552/edpl/2017/4/19

Bygrave L A, 'Core Principles of Data Privacy Law' in Bygrave L A (ed), *Data Privacy Law: An International Perspective* (OUP 2014)
DOI: https://doi.org/10.1093/acprof:oso/9780199675555.003.0005

Cho H et al, 'Testing Three Explanations for Stigmatization of People of Asian Descent during COVID-19: Maladaptive Coping, Biased Media Use, or Racial Prejudice?' (2021) 26 (1) Ethnicity & Health 94
DOI: doi. 10.1080/13557858.2020.1830035

De Hert P and Lammerant H, 'Protection of personal data in work-related relations', Study made on behalf of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (*Publications Office* 2013)

de Terwangne C, 'Article 5. Principles relating to processing of personal data' in Bygrave L A, Docksey C and Kuner C (eds), *The EU General Data Protection Regulation (GDPR): A commentary* (OUP Oxford 2020)
DOI: doi. org/10.1093/oso/9780198826491.003.0034

Dzehtsiarou K, *European Consensus and the Legitimacy of the European Court of Human Rights* (CUP 2015)
DOI: https://doi.org/10.1017/CBO9781139644471

Fischer L S, Mansergh G, Lynch J and Santibanez S, 'Addressing Disease-Related Stigma During Infectious Disease Outbreaks', (2019) 13 Disaster Medicine and Public Health Preparedness 989
DOI: https://doi.10.1017/dmp.2018.157

Georgieva L and Kuner C, 'Article 9 Processing of Special Categories of Personal Data' in Bygrave L A, Docksey C and Kuner C (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020)
DOI: https://doi.org/10.1093/oso/9780198826491.003.0038

Gerards J and Senden H, 'The Structure of Fundamental Rights and the European Court of Human Rights' (2009) 7 International Journal of Constitutional Law 619
DOI: https://doi.org/10.1093/icon/mop028

Keane E, 'The GDPR and Employee's Privacy: Much Ado but Nothing New' (2018) 29 King's Law Journal 354
DOI: https://doi.org/10.1080/09615768.2018.1555065

Kloza D and Drechsler L, 'Proportionality has Come to the GDPR', (*The European Law Blog,* 9 December 2020) <https://europeanlawblog.eu/2020/12/09/proportionality-has-come-to-the-gdpr/> accessed 1 September 2021

Kokott J and Sobotta C, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222
DOI: https://doi.org/10.1093/idpl/ipt017

Kranenborg H, 'Art 8 – Protection of Personal Data' in Peers S., Hervey T., Kenner J and Ward A (eds), *The EU Charter Of Fundamental Rights: A Commentary* (Uppl. 2, Hart Publishing 2014)

Lynskey O, 'Deconstructing Data Protection: The "added-value" of a Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569
DOI: https://doi.org/10.1017/S0020589314000244

Mowbray A, *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights* (Hart Publishing 2004)

Nass S, Levit L and Gostin L O, 'Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research' (*National Academies Press,* 2009) <http://www.ncbi.nlm.nih.gov/books/NBK9579/> accessed 28 April 2022

Oaten M, Stevenson R J and Case T I, 'Disease Avoidance as a Functional Basis for Stigmatization' (2011) 366 Philosophical Transactions of the Royal Society B: Biological Sciences 3433
DOI: https://doi.10.1098/rstb.2011.0095

Oriseg C, 'GDPR and Personal Data Protection in the Employment Context' (2017) 3 Labour & Law Issues 1
DOI: https://doi.org/10.6092/issn.2421-2695/7573

Shabani M, Goffin T and Mertes H, 'Reporting, recording, and communication of COVID-19 cases in workplace: data protection as a moving target' (2020) 7 (1) Journal of Law and the Biosciences 1
DOI: https://doi.10.1093/jlb/lsaa008

Stoyanova V, 'The Disjunctive Structure of Positive Rights under the European Convention on Human Rights' (2018) 87(3) Nordic Journal of International Law 344
DOI: https://doi.org/10.1163/15718107-08703003

Suder S, 'Processing Employees' Personal Data during the Covid-19 Pandemic', (2020) 12 (3) European Labour Law Journal (Internet) 1
DOI: https://doi.org/10.1177/2031952520978994

van der Sloot B, 'Legal Fundamentalism: Is Data Protection Really a Fundamental right?' in Leeds R, et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Cham, Springer 2017)
DOI: https://doi.10.1007/978-3-319-50796-5_1

Van Ecke P and Šimkus A, 'Article 88 Processing in the Context of Employment' in Bygrave L A, Docksey C and Kuner C, *The EU General Data Protection Regulation (GDPR): A commentary* (OUP 2020)

Ventrella E, 'Privacy in emergency circumstances: data protection and the COVID-19 pandemic' (2020) 21 ERA Forum 379
DOI: https://doi.10.1007/s12027-020-00629-3

Wagner J and Benecke A, 'National Legislation within the Framework of the GDPR' (2016) 2 European data protection law review 353
DOI: https://doi.org/10.21552/EDPL/2016/3/10

Žuľová J, Švec M and Madleňák A, 'Personality Aspects of the Employee and their Exploration from the GDPR Perspective' (2018) 1 Central European Journal of Labour Law and Personnel Management 68
DOI: https://doi.10.33382/cejllpm.2018.01.05