Is That Lawful? Data Privacy, Monitoring and Fitness Trackers in the Workplace

Philippa COLLINS* & Stefania MARASSI**

Data collected from fitness trackers worn by employees could be very useful for businesses. The sharing of this data with employers is already a well-established practice in the United States, and companies in Europe are showing an interest in the introduction of such devices among their workforces. Our argument is that employers processing their employees' fitness trackers data is unlikely to be lawful under the General Data Protection Regulation (GDPR). Wearable fitness trackers, such as Fitbit and Apple Watch devices, collate intimate data about the wearer's location, sleep and heart rate. As a result, we consider that they not only represent a novel threat to the privacy and autonomy of the wearer, but that the data gathered constitutes 'health data' regulated by Article 9. Processing health data, including, in our view, fitness tracking data, is prohibited unless one of the specified conditions in the GDPR applies. After examining a number of legitimate bases which employers can rely on, we conclude that the data processing practices considered do not comply with the principle of lawfulness that is central to the GDPR regime. We suggest alternative schema by which wearable fitness trackers could be integrated into an organization to support healthy habits amongst employees, but in a manner that respects the data privacy of the individual wearer.

Keywords: Fitness Trackers, GDPR, Privacy, Data Protection, Employment, Principle of Lawfulness, Fitbit, Apple Watch

1 INTRODUCTION

In February 2019, the CEO of Fitbit told CNBC that 6.8 million individuals wear Fitbit devices as part of corporate wellness programmes, be it through an

* Lecturer in Law, University of Bristol, UK. Email: philippa.collins@bristol.ac.uk. The authors would like to thank the Research Group on the Changing Role of Europe at The Hague University of Applied Sciences for inviting the authors to present their preliminary findings at a CREUVENT workshop on the theme of 'Europe in Working Practice'. We are also grateful to Lauriane Eudeline for her excellent research assistance and to Dr Natasha Dunn for her thoughtful input into section 5. The authors would also like to thank Dimitrios Kagiaros, Naomi Hawkins, Séverine Saintier, Lilian Edwards, Ana Beduschi, Antonio Aloisi, Isabel Plets and the journal's reviewers for their insightful comments. The usual disclaimers apply.

** Lecturer in European and International Labour Law, The Hague University of Applied Sciences, the Netherlands. Email: s.marassi@hhs.nl.

Collins, Philippa & Marassi, Stefania. 'Is That Lawful? Data Privacy, Monitoring and Fitness Trackers in the Workplace'. *International Journal of Comparative Labour Law and Industrial Relations* 37, no. 1 (2021): 1–31.

employer, a health care provider or other commercial entity.[1] Big name brands such as BP, IBM, and Barclays provide wearable devices to thousands of their staff in the hope of changing their lifestyle habits.[2] Insurers and corporate wellbeing programmes in Europe integrate devices such as Fitbits to track the workforce's activity levels.[3] New wearable technology is also emerging apace, designed to improve well-being or increase productivity. For example, the design and deployment of a tracking wristband by Amazon, used in its fulfilment centres in the UK, has been reported.[4] ProGlove wearables AQ1 are being used in IKEA distribution centres to improve worker efficiency.[5] Firstbeat, originally a Finnish company,[6] has designed heart-rate variability sensors and data analytics packages that have been made available to employers across Europe to monitor the physical and mental well-being of their staff.[7] Technology by the UK company BioBeats is intended to reduce stress-related work absences to zero.[8] Their wristband device, the BioBeam, has been used by companies such as WPP Health Practice,[9] AXA Insurance and BNP Paribas.[10] The recent coronavirus pandemic has intensified employers' interest in the health data of their employees, as the population negotiates the return to office spaces and daily contact with colleagues. Initial reports from studies investigating whether wearables such as the Apple Watch can be used as 'early warning systems' for Covid-19 symptoms are reporting success.[11]

---

1 Christina Farr, *Fitbit Has a New Health Tracker, But You Can Only Get It Through Your Employer or Insurer*, CNBC (8 Feb. 2019), https://www.cnbc.com/2019/02/08/fitbit-releases-insprire-for-employers.html.

2 Christina Farr, *How Fitbit Became the Next Big Thing in Corporate Wellness*, Fast Company (18 Apr. 2016), https://www.fastcompany.com/3058462/how-fitbit-became-the-next-big-thing-in-corporate-wellness.

3 *See*, e.g., The Guardian, *Wearables Could Make It Impossible to Keep Your Hangover Secret at Work* (30 Sept. 2015), https://www.theguardian.com/sustainable-business/2015/sep/30/wearables-companies-smart-devices-health-wellbeing-privacy; Cmonassurance, *Entreprise: et si des bracelets Fitbit pouvaient diminuer vos frais d'assurance?*, https://www.c-mon-assurance.com/actualites/mutuelle-entreprise/offrir-des-bracelets-fitbits-a-ses-employes-le-pari-gagnant-pour-diminuer-ses-frais-dassurance/, and 10.000 stappenplan, https://www.10000stappen.nl/bedrijven (with the use of the pedometer Yamax EX-210).

4 Phoebe Moore, *The Quantified Self in Precarity: Work, Technology and What Counts* 163–164 (Book 229 *Routledge Advances in Sociology* 2017).

5 RIS News, *IKEA Expands Use of Wearables in Its DCs* (22 May 2019), https://risnews.com/ikea-expands-use-wearables-its-dcs#close-olyticsmodal.

6 *See* https://www.firstbeat.com/en/company/story/.

7 *See* https://www.firstbeat.com/en/wellness-services/firstbeat-life-corporate-wellness/.

8 Jamie Bell, *BioBeats Technology Cuts Number of Stress-Related Work Absences to Zero in Study*, NS Healthcare (21 Feb. 2020), https://www.ns-healthcare.com/news/biobeats-mental-health-employee-absences/.

9 BioBeats, *WPP Health Practice Adopts New Digital Health Technology*, Medium (13 Dec. 2019), https://medium.com/@biobeats/wpp-health-practice-adopts-new-digital-health-technology-1d4e78a512e1.

10 David Plans, *Stress-busting App Keeps Employees Healthy – and Boosts Productivity*, MedTech Views (1 Mar. 2017), http://www.medtechviews.eu/article/stress-busting-app-keeps-employees-healthy-%E2%80%93-and-boosts-productivity?page=1.

Whilst wearable fitness trackers[12] may be useful in monitoring employee health and wellbeing, would an employer's processing of such data be in accordance with the European principles of data protection? In this article, we argue that sharing data from an activity tracker with one's employer is unlikely to pass scrutiny under the General Data Protection Regulation (hereinafter GDPR or the Regulation).[13] The deployment of such devices in the workplace, a setting characterized by an imbalance of power between the parties, raises a number of privacy, autonomy and data protection-related concerns (section 2). The GDPR plays an important role in limiting employers' collation and analysis of tracker data. Even before the GDPR entered into force, the Dutch data protection authority shut down a pilot study run by a business that collected data from its employees' Fitbits.[14] This decision was made on the grounds that employers could not rely upon their employee's consent to legitimize processing their sensitive data.[15] Our contention is that, in most cases, the processing by employers of employee data sourced from fitness trackers breaches the GDPR. Less invasive methods must be substituted in order to achieve compliance with data protection principles, which we discuss in section 7.

Our central argument focuses upon the first barrier in designing a GDPR-compliant data processing regime: lawfulness. Fitness trackers enable employers to monitor intimate data, such as level of daily activity, sleep quantity and quality and heart rate variability, around the clock. We argue that the metrics produced by fitness trackers amount to personal health data as described and regulated by the GDPR, giving specific examples of "diagnoses" that employers could derive from an analysis of an employee's device data (section 5). Processing this data is therefore prohibited unless it falls within the strictly limited exceptions contained in Article 9 GDPR.

In sections 6&7, we focus our analysis on specific routes, set out by the GDPR, that employers may rely upon to render their processing of activity tracker data lawful.

---

11 Geoffrey A. Fowler, *Wearable Tech Can Spot Coronavirus Symptoms Before You Even Realize You're Sick*, Washington Post (28 May 2020), https://www.washingtonpost.com/technology/2020/05/28/wearable-coronavirus-detect/; *see also* Conor Heneghan, *Early Findings from Fitbit COVID-19 Study Suggest Fitbit Devices Can Identify Signs of Disease at Its Earliest Stages*, Fitbit (19 Aug. 2020), https://blog.fitbit.com/early-findings-covid-19-study/.

12 Devices that fall into the category considered in this article include the Apple Watch, the Garmin Vivosmart 4, the Huawei Band 3 Pro, and Fitbit Charge and Fitbit Inspire products, as they have similar capacities such activity and sleep tracking, a GPS element and heart rate monitoring which will be analysed below in s. 4.

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 (4 May 2016).

AQ3 14 Autoriteit Persoonsgegevens (Dutch Data Protection Authority), *AP: Verwerking gezondheidsgegevens wearables door werkgevers mag niet* (8 Mar. 2016), https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet.

15 *Ibid*.

Given the sensitive character of the employee data collected with fitness trackers, in section 6 we focus predominantly on Article 9 exceptions, while also examining any Article 6 lawful bases that may be applicable. We consider consent and a number of purpose-specific provisions, highlighting in particular the challenge posed by the GDPR concept of necessity when applied to wearable fitness trackers in the workplace, due to the risk of the employer over-collecting data.

In order to offer substantial and definite analyses of the lawfulness of tracker monitoring, we devise and assess two potential models for integrating wearable fitness trackers into a workplace. They are based on the existing practices and likely practices of employers in deploying fitness trackers and other wearables in the workplace. The first model (Wellness Model) is based on a general concern for staff health and wellbeing, seeking to prompt and incentivize healthy habits among the workforce. In contrast, the second model (Performance Management Model) uses data from activity trackers for performance management purposes, assessing capability, monitoring productivity and even supplementing investigations into misconduct. The nuances of these models affect the likelihood of their lawfulness, and we argue that both processing regimes would face difficulties establishing a legitimate basis under the Regulation.

This article builds on the current debate in labour law doctrine about the development and introduction of algorithm-driven technologies in the workplace and the privacy-related implications.[16] In contrast to an analysis showing that practices such as these are essentially unregulated in the United States,[17] we demonstrate that the GDPR has an important role to play in shaping attempts to monitor individuals at work. The principles of data protection are at the heart of the alternative solutions that we present in section 8. These alternatives would allow employers to support their workforce in using wearable fitness trackers while ensuring that data protection principles are complied with and privacy and autonomy concerns are minimized. We thereby offer the first thorough analysis of data processing practices relating to wearable fitness trackers, contextualized by the insights of labour literature and directly translatable into organizational policies.

[16] For example, see the contributions in Comp. Lab. L. Pol'y J., 41 Automation, Artificial Intelligence, Lab. L. (2019); Frank Hendrickx, *From Digits to Robots: The Privacy-Autonomy Nexus in New Labor Law Machinery*, 40(3) Comp. Lab. L. & Pol'y J. 365 (2019); Bart Custers & Helena Ursic, *Workers Privacy in a Digitalized World Under European Law*, 39(2) Comp. Lab. L. Pol'y J. 323 (2018); and Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105(3) Cal. L. Rev. 735 (2017).

[17] Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16(1) Yale J. Health Pol'y L. Ethics 1 (2016).

2 FITNESS TRACKERS IN THE WORKPLACE: AN ADDITIONAL THREAT TO AUTONOMY AND PRIVACY?

As every new technology is deployed in the workplace, it seems that new challenges and risks appear. Here we focus on two concerns about the use of fitness trackers in the workplace: privacy and autonomy. In relation to privacy, there are three novel concerns about the use of fitness trackers in the workplace and the sharing of data gathered: bodily integrity, 24/7 monitoring and the work-life boundary, and the sensitive nature of the data shared. The first concern is the *wearable* nature of the device. Other forms of monitoring and tracking performed electronically may be by means of a laptop or mobile. A wristband activity tracker, however, is a device that must be worn by the employee. Physical bodily integrity is therefore relevant to discussions about fitness devices, in addition to concerns about informational or behavioural privacy. At its most basic, requiring an employee to wear a device would amount to an invasion of that individual's right to bodily integrity if not accompanied by appropriate consent.

Secondly, the use of a fitness tracker puts further pressure on the already porous boundary between work life and private life. In order for such a device to be most effective in monitoring the individual, it should be worn 24 hours a day, seven days a week. If we previously thought that working hours placed notional confines on the employer's control and influence over the workforce, 24/7 monitoring of an individual's location, activity, sleep and heart rate would erase these limitations. An employee sharing health and activity data gathered via a fitness wristband with their employer would accelerate the abandonment of any divide between work and private life.

As will be discussed further below, the final privacy concern relates to the expansion of the type of data being collected by the employer. In a 2015 survey, 52% of employees expressed a concern about the amount of personal data that employers are able to access via wearable technology.[18] Devices such as a Fitbit or a Garmin smartwatch take raw data from the device's accelerometer, heart rate sensor, altimeter and location services and apply the manufacturer's algorithms to calculate or, more precisely, *estimate* information such as the wearer's step count and other forms of activity undertaken, the calories burned, the heart rate zones, the amount and quality of his/her sleep, and so on. Whereas previously employees would have had control over whether and when this kind of information was shared with their employer, monitoring via fitness trackers would remove that choice.

Strongly connected to these potential privacy infringements, monitoring via wearable fitness trackers also raises concerns for the exercise of autonomy by

[18] ADP UK, *Putting Wearables to Work – New Technology Could Revolutionise the Workplace*, Personnel Today, Technology (14 July 2015), www.personneltoday.com/pr/2015/07/putting-wearables-to-work-new-technology-could-revolutionise-the-workplace/.

employees. Autonomy can be broadly conceived to incorporate both negative freedom from interference by others (state or private actors) and a positive right to self-determination, to choose how to live one's life.[19] One could argue that participating employees are exercising their autonomy in *choosing* to share their data with their employer, in *choosing* to know more about themselves and in *choosing* to seek to improve their wellbeing, health or performance at work. This argument has been questioned by labour and human rights law scholars, as well as data protection authorities.[20] As observed by Willborn, the consensus reached is that 'consent within the employment relationship is compromised' and arguments based on employee consent must be treated with scepticism.[21]

Take the reported use of activity and health trackers at Buffer, an American social media start-up, by way of example. A wearable device was offered to all employees and their sleep tracking data was shared between colleagues, as well as being used to screen internal promotion applications. While uptake of the device was not mandatory, the company's chief happiness officer reported that no-one had refused the device or the monitoring.[22] When asked about the position of individuals who might be uncomfortable with the use of data in this way in 2014, the company's chief happiness officer responded that those individuals 'might not fit into Buffer's culture in the first place'.[23]

The example of Buffer's monitoring and sharing regime allows us to unpick a number of autonomy concerns. The quality of consent given, in a context that has been described as one of submission and subordination,[24] must be open to doubt. Workers rely on their job as a source of income, among many other important interests, and therefore any request made within that relationship is tainted by an imbalance of power and a sense of dependence. This question is pursued in detail in section 6.1. Combine this vertical relationship with the social pressure that may be felt horizontally from colleagues and we arrive at a situation where even non-mandatory policies are implemented across the entire workforce. Employers may also use financial resources or other incentives, such as the offer of reduced healthcare premiums, to further shape the choices made by their employees. If invasive monitoring practices become the norm, it will become difficult, and

19 James Griffin, *On Human Rights* ch. 8 (Oxford University Press 2008).
20 *See* section 6.1 *infra*.
21 Steven L. Willborn, *Consenting Employees: Workplace Privacy and the Role of Consent*, 66 La. L. Rev. 975, 976 (2006).
22 Siraj Datoo, *These Companies Are Tracking the Fitness of Their Employees*, The Guardian (17 Mar. 2014), https://www.theguardian.com/technology/2014/mar/17/why-companies-are-tracking-the-fitness-of-their-employees.
23 David Nield, *In Corporate Wellness Programs, Wearables Take a Step Forward*, Fortune (15 Apr. 2014), https://fortune.com/2014/04/15/in-corporate-wellness-programs-wearables-take-a-step-forward/.
24 Paul Davies & Mark Freedland, *Kahn-Freund's Labour and the Law* 18 (Stevens 3d ed. 1983).

potentially a source of discrimination,[25] for employees to exercise their autonomy in choosing *not to* wear a fitness tracker and to *avoid* sharing extensive data with their employer and possibly even their colleagues.

3 THE WELLNESS MODEL AND THE PERFORMANCE MANAGEMENT MODEL

Against this background, this article discusses two models of implementation that organizations could use in integrating fitness tracking devices into their workplace: the Wellness Model and the Performance Management Model. In devising these models, we draw upon schemes that are reported either in the media or in company websites about the deployment of fitness trackers or other types of wearables in the workplace. The most established monitoring practices are seen in the US, though the development of workplace wearables and corporate experimentation with their application is growing in Europe. This increased interest is demonstrated by the range of examples cited throughout this article.

In the Wellness Model, the wearable is used as part of a wider (voluntary) corporate wellbeing programme.[26] Here, the employer's main reason to introduce such a device is a general desire to monitor workers' health and wellbeing with a view to supporting healthy lifestyle habits.[27] This model seems to dominate in larger corporations that possess the resources to invest in the technology and support the scheme. The employee is given a smartwatch to track his/her activity levels and habits and that data is shared with the employer, who monitors the employee's progress. This data monitoring is the focus of our analysis, but other common elements are: a subsidy on the price of the smartwatch, bonuses for achieving particular milestones and inter-colleague or team-based competitions within the workplace. On the surface, the motivation for the data sharing and accompanying measures is to improve employee wellbeing. However, as will be elaborated upon further below, it is difficult to delineate motivations clearly. A healthy workforce is more likely to be a productive one, and distinct purposes thereby blur into each other. Nevertheless, we will separate health and wellbeing

[25] Janine Berg, *Protecting Workers in the Digital Age: Technology, Outsourcing, and the Growing Precariousness of Work*, 41(1) Comp. Lab. L. Pol'y J. 69, 80 (2019).

[26] *See also* Céline Brassart Olsen, *To Track or Not to Track? Employees' Data Privacy in the Age of Corporate Wellness, Mobile Health, and GDPR*, 10(3) Int'l Data Privacy L. 36, 236, 238–239 (2020).

[27] An employer could also deploy wearable devices to comply with the general duty of care as required under European and national occupational health and safety legislation. The occupational health and safety perspective raises interesting questions but is beyond the scope of this article as it introduces a further layer of regulation in the form of regional and national health and safety obligations. Some of these issues are addressed by Emanuele Dagnino, *Dalla fisica all'argoritmo: una prospettiva di analisi giuslavoristica* 137–141 (ADAPT University Press 2019).

from productivity and efficiency concerns, which are more directly connected to the Performance Management Model below.

A number of wellness programmes advertised by employers or the companies that support them would fit within this model. In the US, BP offered Fitbit step counters to its workforce as an element of its health and wellbeing strategy, reporting a voluntary uptake of 90% across its staff.[28] Closer to home, in 2015, media reports stated that '75,000 employees in the US and UK across the investment bank [Barclays] … will have the chance to buy a subsidised Fitbit' as part of a new wellness initiative.[29] Several companies in the UK and the Netherlands have experimented with using smartwatches to combat stress at work and measure resilience among the workforce.[30] External companies may also incentivize the use of smartwatch monitoring. For example, French providers of corporate health insurance have advertised the use of Fitbits as a way of businesses reducing their insurance costs,[31] and a wearable may be included in a corporate wellness package such as Virgin Pulse.[32] The reports do not go into detail regarding the data sharing practices deployed. However, it appears that, for most schemes, the device data is stored by the employer along with other wellbeing data, such as employee self-assessments, and both the employee and relevant teams within the organization, such as Occupational Health or the Human Resources team, can access a personalized hub of information about the employee-wearer's wellbeing and progress.

In the Performance Management Model, wearing a fitness tracker is a mandatory obligation placed upon employees. This model, seen most prominently in start-up enterprises with a strong culture of transparency and the use of technology, has appeared in various forms, using a range of wearable devices and tracking software. Some employers require their workers to install apps on their mobiles which track the individual's location 24/7.[33] Amazon's development of its own

---

[28] Jessica Grossmeier & Chris Phalen, *How BP Found Success with Wearables*, Employee Benefit News (24 Aug. 2017), https://www.benefitnews.com/opinion/how-bp-found-success-with-wearables?tag=00000151-16d0-def7-a1db-97f036970000; Jared Lindzon, *What Industries Are the First to Introduce Wearables at Work? Fast Company* (29 Sept. 2014), https://www.fastcompany.com/3036331/what-industries-are-the-first-to-introduce-wearables-at-work.

[29] Parmy Olson, *Fitbit on Track to Sells Thousands More Devices Through Barclays, GoDaddy and Other Employers*, Forbes (25 Oct. 2015), https://www.forbes.com/sites/parmyolson/2015/10/20/fitbit-employers-barclays-godaddy-wellness/.

[30] Heather Mack, *BioBeats Announces Results of Study with BNP Paribas, Looks to Expand Wellness Coaching Platform*, Mobile Health News (6 Oct. 2016, 02:02 am), https://www.mobihealthnews.com/content/biobeats-announces-results-study-bnp-paribas-looks-expand-wellness-coaching-platform; For a Dutch pilot, *see* Moore, *supra* n. 4, at 166ff.

[31] Cmonassurance, *supra* n. 3.

[32] Virgin Pulse packages integrate activity trackers such as Fitbits, mobile apps and online platforms into existing workplace wellness programmes, https://www.virginpulse.com/en-gb/our-wellbeing-solutions/.

[33] *See* the case (later withdrawn) and coverage of *Arias v. Intermex Wire Transfer:* Adriana Gardella, *Employer Sued for GPS-Tracking Salesperson 24/7*, Forbes (5 June 2015), https://www.forbes.com/sites/adrianagardella/2015/06/05/employer-sued-for-gps-tracking-salesperson-247/; Ajunwa Ifeoma,

smart wristbands, designed to give haptic feedback when an employee performs a task inefficiently, for use by its workforce has been reported.[34] In the Amazon warehouse in Swansea (UK), 'pickers' use a wearable device that instructs them on what to collect and the required completion time. In a Tesco warehouse in Ireland, factory workers wore a wristband to find and collect goods.[35] In 2014, there were reports of a UK company adopting extensive mandatory activity, sleep and diet tracking across their workforce.[36] These instances indicate an appetite among employers for the mandatory use of wearable technologies to track the activity, movement and location of their workforce.

A mandatory programme of data collection could be deployed for a number of purposes related to employee performance management. We include within our definition scrutinizing productivity and output, detecting potential misconduct, and monitoring the employee's working capabilities. Data collected by a fitness monitoring device could be included in investigations into employee misconduct or poor performance and contribute to an employer's decision to discipline or even dismiss an employee. Table 1 provides an overview of the key features of the Wellbeing Model and the Performance Management Model.

AQ2

Table 1 Key Characteristics of the Wellbeing Model and the Performance Management Model

	Wellbeing Model	*Performance Management Model*
Participation	Self-selection by employees, employees can opt-out	Mandatory for designated employees
Access to data	Employee, *and* Occupational Health or Wellbeing team, *and* Human resources	Employee, *and* Line managers, *and* Team leaders
Purpose of processing	Monitoring overall staff health and wellbeing to	Performance management

Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law, 63(1) St. Louis U. L.J. 21, 25ff (2018).

34 Ceylan Yeginsu, *If Workers Slack Off, the Wristband Will Know (And Amazon Has a Patent for It.)*, The New York Times (1 Feb. 2018), https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html.

35 Moore, *supra* n. 4, at 163–164.

36 Datoo, *supra* n. 22.

	Wellbeing Model	*Performance Management Model*
	encourage healthy lifestyle habits	

Source: Authors' own elaboration.

4 GDPR AND FITNESS TRACKERS IN THE WORKPLACE

This article focuses on employers in their strategic role as data controllers.[37] Data controllers determine the purpose, means and confines of data collection from the workforce and are responsible for ensuring compliance with the Regulation's principles, which should be integrated into the design phase of any data processing programme.[38] This section will present an overview of the applicability of the Regulation and some other key principles that a data controller would have to consider before embarking on fitness tracker data monitoring.

The GDPR is applicable to a significant number of employers as a result of its wide territorial scope. Importantly, any data controller (or processor) that is established within the EU is covered,[39] and the GDPR also applies to any processing of data where the data subject is within the EU.[40] EU statistics show that, in 2019, 190,914,000 people were employed across the twenty-eight EU Member States.[41] Each individual would be a data subject for the purpose of the GDPR. Any data processing that monitors the activities of these millions of workers while they are in the EU must comply with GDPR.[42] The territorial scope of the Regulations will thus impact employee monitoring by a huge number of data controllers based within and outside the European Union.

As the data controller, an employer must demonstrate compliance with the general principles and rules set out in the GDPR.[43] Specifically, Article 5 lists six core principles that the data controller is accountable for when processing personal data. While all principles would have implications for the design of a wearable fitness tracker monitoring programme, this section will highlight three principles of particular interest: purpose limitation, data minimization and data accuracy.[44]

37 Article 4(7) and Recital 74 GDPR.
38 Article 25 GDPR.
39 Article 3(1) GDPR.
40 Article 3(2). This route is available only in relation to the processing in the context of specific activities listed in this provision.
41 Eurostat, https://ec.europa.eu/eurostat/web/lfs/data/database.
42 Article 3(2)(b) GDPR.
43 Eduardo Ustaran, *European Data Protection Law and Practice* 74ff (International Association of Privacy Professionals 2018).

The purpose limitation principle entails two sub-principles: purpose specification and use limitation. A data controller must specify, in advance, a 'specified, explicit and legitimate purpose' for the data processing.[45] The regulation of legitimate purposes is undertaken by the lawfulness principle, discussed below, which sets out a finite list of purposes in pursuit of which data may be processed. In principle, maintaining staff health and wellbeing and monitoring the productivity of the employees of the business could be argued to be legitimate purposes, linked as they are to sustaining efficiency within an enterprise,[46] a major concern for any employer.

Secondly, the employer cannot further process the set of data in a way that is incompatible with the initial purpose.[47] Ensuring and assessing compliance with the use limitation sub-principle is particularly challenging in our case, as the purposes outlined above may blur into one another. For example, the project run by a Dutch company that analysed Fitbit data, RescueTime data (a productivity app), and employee self-assessments was designed to monitor employees during a period of change. The stated goals of the monitoring demonstrate how closely linked and overlapping an employer's aims can be: they sought to monitor employee stress levels, wellbeing and 'wellbilling' (the amount of revenue an employee generates for the company).[48] The company had realized that a lack of wellbeing is likely to impact on productivity and that it is difficult to isolate these factors from each other. Therefore, the demand made by the purpose limitation principle that an employer only processes data for one stated purpose *and no others* is challenging to comply with in the case of fitness tracker monitoring.

The principle of purpose limitation is firmly connected to the principle of data minimization, which limits the amount of data that can be processed to that which is '*necessary* in relation to the purposes for which they are processed'.[49] For example, to comply with this principle in the Wellbeing and the Performance Management Models, the employer would need to demonstrate that the volume of data collected regarding sleep patterns, step counts, heart rate variability and many

---

44 The other principles are: lawfulness, fairness and transparency, storage limitation, integrity and confidentiality. ss 5 and 6 will discuss the lawfulness principle. Given the limited space, this article will not examine the remaining principles.

45 Article 5(1)(b) and Recital 39 GDPR. *See also* Art. 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN, WP2013, Adopted on 2 Apr. 2013; Custers & Ursic, *supra* n. 16, at 332 and 337–38.

46 Moore, *supra* n. 4, at 167.

47 WP 29, Opinion 3/2013, *supra* n. 45, at 12 and 20ff; *see also* Frank Hendrickx, *Article 8 Protection of Personal Data* 266 (Filip Dorssemont et al. eds, *The Charter of Fundamental Rights of the European Union and the Employment Relation*, Hart 2019).

48 Moore, *supra* n. 4, at 167.

49 Article 5(1)(c) GDPR [emphasis added]. *See also* European Data Protection Supervisor, Glossary, Data minimization, https://edps.europa.eu/data-protection/data-protection/glossary/d_en.

other metrics is both suitable and not excessive to infer information about the overall mental and physical wellbeing of an employee or his/her productivity, respectively.[50] another important factor in this assessment is whether alternative means of data processing that are less privacy-invasive could be used.[51] Thus, even if tracking sleep patterns could indicate lower productivity or provide information about an employee's mental health, an employer should evaluate whether less privacy-invasive monitoring could achieve the same purpose.

Compliance with the data accuracy principle could also be challenging for employers who make decisions or recommendations that rely on wristband tracking data.[52] For example, a review of fifty-seven studies of the accuracy of Fitbit data concluded that discretion should be exercised when using Fitbits in research or health-care contexts as 'there are seemingly a limited number of situations where the device is likely to provide accurate measurement'.[53] While the accuracy of the data from wearable fitness devices will likely improve over time, relying on data that the employer knows to contain inaccuracies would be in breach of the Regulation as 'every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted'.[54]

Although all these considerations are essential in designing a compliant data processing regime, the first hurdle for any data controller is demonstrating the lawfulness of their processing. Article 6 states that '[p]rocessing shall be lawful only if and to the extent that at least one of the following [lawful bases] applies'.[55] The lawfulness principle therefore places a strict boundary on data processing: go beyond these legitimate bases offered by the Regulation and the activity will be unlawful. The remaining sections are dedicated to analysing whether an employer who has adopted either model set out above would be able to comply with the principle of lawfulness as set out in Articles 5(1)(a) and 6 GDPR.

5 DATA DERIVED FROM FITNESS TRACKERS: PERSONAL DATA AND HEALTH DATA?

Our first task is to evaluate precisely what type of data an employer, *qua* data controller, would be collecting and processing under the Wellness and Performance Management models above. There are two questions that must be

---

50 Ustaran, *supra* n. 43, at 106–07.
51 *Ibid.*, at 106; *see also* Recital 39 GDPR.
52 Article 5(1)(d) GDPR.
53 Lynne M. Feehan et al., *Accuracy of Fitbit Devices: Systematic Review and Narrative Syntheses of Quantitative Data*, 6(8) JMIR Mhealth Uhealth e10527 (2018), https://mhealth.jmir.org/2018/8/e10527/.
54 Recital 39 GDPR.
55 Article 6(1) GDPR. The six legal bases are: consent, contract performance, compliance with legal obligations, vital interest of individuals, public interest, and legitimate interest.

addressed here: is the data collected by a wristband personal data to which GDPR applies? Further, is any of the data that an employer would collect and process from this wearable device within the special categories of data regulated by Article 9 GDPR? Below, we argue that some of the data collected by a fitness tracker concerns health.

5.1 Personal data

The broad definition of personal data to which the GDPR applies is found in Article 4(1).[56] Such data is defined as 'any information relating to an identified or identifiable natural person'.[57] An employer could consider accessing data on an aggregate basis, meaning that an individual's data should not be identifiable and could not be analysed separately. Some wellbeing programmes may adopt this approach. However, de-anonymized data would be the preferred choice for an employer seeking to monitor wellbeing or performance on an individual basis.

To set up an account and run a fitness tracking device, the wearer must share a wide range of information about themselves. The individual's name, email address and data of birth are required to set up an account, and location data is collected from the device and linked to the account whenever the individual is wearing it. The sensors also generate information about number of steps, calories burned, 24-hour heart rate, sleep stages, distance travelled, and so on. This type of information is all personal data and, if shared with an employer, would result in the GDPR being applicable. Further, the threshold for *processing* such data under the GDPR is low: any retrieval, consultation, storage, or combination of personal data is covered by the GDPR.[58] Any regime under which the employee's device data is stored, analysed or examined by the employer would constitute processing to which the GDPR, and particularly the principle of lawfulness, applies.

5.2 The GDPR definition of health data

The classification of the data collected via a wearable device as health data is crucial as it would add a further layer of regulation given the sensitive nature of this information. Any processing of data concerning health is prohibited under the GDPR unless an enumerated exception applies.[59] The European legislator's

[56] Hendrickx, *supra* n. 47, at 259.
[57] Article 4(1) GDPR.
[58] Article 4(2) GDPR.
[59] Article 9(1) and Recitals 50–51 GDPR.

definition of health data is wide.[60] According to Article 4(15), health data is 'personal data related to the physical or mental health of a natural person (…) which reveal information about his or her health status'.[61] The Regulation's preamble specifies that the information may relate 'to the past, current or future physical or mental health status of the data subject'.[62] What criterion can then be applied to draw the boundary of health data under the GDPR?

The Article 29 Working Party established under the 1995 Directive (hereinafter, the Working Party) gave guidance as to when the data collected by lifestyle and wellbeing devices and apps falls *within* the category of health data.[63] Given the similarities in phrasing and legislative design, it is assumed that this guidance still holds persuasive value under the GDPR. In addition to 'inherently/clearly medical data',[64] the Working Party stated that health data includes 'raw sensor data that can be used [by] itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person'.[65] More generally, and crucially for this article, data regarding health includes whenever '[c]onclusions are drawn about a person's health status or health risk (irrespective of *whether these conclusions are accurate or inaccurate, legitimate or illegitimate, or otherwise adequate or inadequate*)'.[66]

It is against this background that one must consider how conclusions may be drawn about a worker's health status and disease risk on the basis of the data collected and analysed by the wearable technology.[67] We argue that such conclusions could be derived in three situations that are explored below: (1) a fitness tracker's standard metrics are health data; (2) analysis of the metrics over time could lead to conclusions about health status, and (3) conclusions reached through a combination of tracking data and other data would qualify as health data.

5.3 Three routes to a health data classification

There are many different types of data that a device wearer can access about themselves. Most devices rely on measurements from three elements: a three-dimensional accelerometer system which tracks motion, including its frequency,

---

60 Tal Z. Zarsky, *Correlation Versus Causation in Health-Related Big Data Analysis*, in *Big Data, Health Law, and Bioethics* 44–46 (Glenn Cohen et al. eds, Cambridge University Press 2018).

61 Article 14(5) GDPR.

62 Recital 35 GDPR.

63 Olsen, *supra* n. 26, at 243–244.

64 Article 29 Data Protection Working Party, Letter to the European Commission *Annex – Health Data in Apps and Devices* (2015).

65 *Ibid.*, at 5.

66 *Ibid.* [emphasis added].

67 Article 29 Data Protection Working Party (WP 29), Opinion 2/2017 on data processing at work, 17/EN, WP 249 Adopted on 8 June 2017, at 17–18; T. Mulder & M. Tudorica, *Privacy Policies, Cross-border Health Data and the GDPR*, 28(3) Information Comm. Tech. L. 261, 263–65 (2019).

duration and intensity; an altimeter which measures elevation, and an optical heart rate sensor. The manufacturers have developed algorithms that use this data to estimate a number of metrics such as number of steps, heart rate variability, sleep stages, active time and location. Of this raft of metrics, we concentrate mainly on three health and exercise features which are recorded by a number of different brands of tracker: sleep tracking, steps and activity tracking, and 24/7 heart rate tracking.

As soon as the employee-wearer has set up an account and worn the device for one day, the employer would have access to some health data. Account data inputted by the user alone could constitute such data. For example, weight could indicate that the individual is overweight or obese. The measured metrics, after only a brief period of tracking, could provide information from which the employer could draw further conclusions about health status, whether accurate or not. Sleep tracking data could generate a 'diagnosis' of insomnia or hypersomnia,[68] and similarly the heart rate data could prompt conclusions regarding bradycardia (slow heart rate), tachycardia (rapid heart rate) or other irregularities in heart rate.[69]

Tracking the metrics over time adds a further set of potential health-related conclusions. For example, a sedentary lifestyle is associated with a number of health risks for the individual.[70] In addition, once the 'norm' for an individual wearer has been established, data showing deviation from that norm could be taken to indicate a health condition. For example, periods of increased heart rate and a decrease in the amount or quality of sleep could lead to a conclusion that the wearer is experiencing anxiety or stress.[71] An unusually sedentary period with limited activity and movement may be believed to indicate a period of depression.[72] These conclusions would constitute health data whether or not the metric inputted was accurate or the conclusion reached was valid.

Such conclusions about health status or health risks may be expedited or confirmed by combining tracking data with other data to which the employer has access. For example, attendance and absence records for an individual could confirm an employer's conclusion that the worker is suffering from a physical or mental health condition. Social media profiles can give insight into the mental wellbeing of the individual,[73] as well as traditional performance management reviews or the individual's use of occupational health services. By drawing together

---

68 Andrew M. Colman, *A Dictionary of Psychology* (Oxford University Press 2014) 'Dyssomnias'.

69 Ian B. Wilkinson et al., *Oxford Handbook of Clinical Medicine* 98, 122 and 124 (Oxford University Press 10th ed. 2017).

70 Aoife Stephenson et al., *Using Computer, Mobile and Wearable Technology Enhanced Interventions to Reduce Sedentary Behaviour: A Systematic Review and Meta-analysis*, 14(1) IJBNPA 105 (2017).

71 Colman, *supra* n. 68, 'Generalised Anxiety Disorder'.

72 *Ibid.*, 'Major depressive episode'.

and analysing all of this data, the employer can make suppositions about current health status or emerging health risks. Thus, in addition to analysis over time producing health data, the combination of device data with other information accessible to the employer could generate conclusions about a worker's health.

Given the breadth of the definition of health data and the three clear routes through which an employer could generate conclusions, accurate or inaccurate, about his/her employees' health, we argue that the employer is processing health data in both the Wellness and the Performance Management model.

6 THE LAWFULNESS PRINCIPLE: THE SCOPE OF THE ARTICLE 9 EXCEPTIONS

Once it is established that, under either model of implementing fitness trackers in the workplace, the employer would be processing health data, the applicability of one of the exceptions to the prohibition to process sensitive data under Article 9 must be demonstrated. We focus on the most likely options in an employment context: consent (Article 9(2)(a)); necessary to comply with the obligations in the field of employment law (Article 9(2)(b)); and necessary for occupational medicine and to assess the working capacity of the employee (Article 9(2)(h)). Should any of these exceptions apply, the employer will also need to identify a legitimate legal basis under Article 6, which will be discussed in Section 7.[74]

6.1 Consent as an unlikely legal basis

In the case of sensitive data under Article 9, consent must be explicitly given.[75] This is in addition to the cumulative requirements[76] laid down in Article 6 for consent to be accepted as a legitimate basis: 'freely given, specific, informed and unambiguous'.[77] But would consent to data processing given by an employee to his/her employer in the context of the Wellness or Performance Management Models be accepted as a legitimate legal basis? Our argument here is that, under the current European data protection regime, it is improbable that employers would be able to rely on consent to process their

---

73 Leora F. Eisenstadt, *Employer or Big Brother? Data Analytics and Incursions into Workers' Personal Lives* 167–168 (Tindara Addabbo et al. eds, *Performance Appraisal in Modern Employment Relations*, Palgrave Macmillan 2019).

74 WP 29, Opinion 2/2017, *supra* n. 67, at 5–6.

75 Ustaran, *supra* n. 43, at 124–125.

76 European Data Protection Board (EDPD), Guidelines 05/2020 on consent under Regulation 2016, Adopted on 4 May 2020, at 5.

77 Article 4(11) GDPR.

employees' activity and fitness data in either of the models. Specifically, we will focus on one of the criteria: freely given.

It is highly unlikely that consent can be freely given by employees due to the relational context in which it is requested. In a relationship that has variously been characterized as one of subordination, control and dependence,[78] we argue that any consent to data processing of this kind would not be truly freely given in the words of the Regulation.[79] An imbalance of power between the two sides renders consent suspect under the GDPR.[80] In this respect, doctrine and the Working Party (and now the European Data Protection Board) noted the likelihood that an employee would feel pressure to consent to processing,[81] reinforcing the concern about the quality of an employee's consent. This factor was key to the Greek Data Protection Authority's decision that PriceWaterhouseCooper's reliance on consent as the legitimate basis for processing their employees' data was inappropriate.[82] We can also see from the Dutch Data Protection Authority's decision regarding the 'quantified-self' pilot, which integrated Fitbit data, that this concern is heightened where the processed data is sensitive health data.[83] In relation to wearable devices such as fitness trackers, the Working Party has gone further, stating that *even if* the employer does not have direct access to employee health data but only through a third party, the concerns about the quality of the consent and the sensitivity of health data mean that it is 'highly unlikely that legally valid explicit consent can be given for the tracking or monitoring of such data'.[84]

This argument stands for both the Wellness and the Performance Management models, being supplemented in the latter by a concern regarding 'bundling' of consent. European data protection guidance makes it clear that it is undesirable to 'bundle' consent into a wider contractual arrangement or to 'tie' the provision of a contract to the data subject giving consent to processing unnecessarily for the performance of that contract. The presumption in these situations is that the consent is not freely given, and therefore cannot be relied on.[85] In the

---

78 Achim Seifert, *Employee Data Protection in the Transnational Company* 180, vol. 100 (Frank Hendrickx & Valerio De Stefano eds, *Game Changers in Labour Law – Shaping the Future of Work*, Wolters Kluwer 2018); European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* 144 (Publications Office of the European Union 2018).

79 Olsen, *supra* n. 26, at 245.

80 Recitals 42 and 43 GDPR.

81 Claudia Ogriseg, *GDPR and Personal Data Protection in the Employment Context*, 3(2) Lab. L. Issues 11 (2017); WP 29, Opinion 2/2017, *supra* n. 67, at 6–7 and 23; EDPD, Guidelines 05/2020, *supra* n. 76, at 9.

82 Hellenic Data Protection Authority's Decision No. 26/2019, for the English summary of the outcome, https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF.

83 Dutch Data Protection Authority, *supra* n. 14; Moore, *supra* n. 4, at 166.

84 WP 29, Opinion 2/2017, *supra* n. 67, at 18.

85 EDPD, Guidelines 05/2020, *supra* n. 76, at 10, referencing Art. 7(4) and recital 43 GDPR.

Performance Management Model, the use of wearable fitness devices is mandatory. If the offer or continuation of a contract of employment is contingent on the employee's consent to the employer's health data processing, the argument that consent could be a legitimate basis for the employer's processing is further undermined.[86] These challenges and concerns about the involuntary nature of employee consent lead us to discard consent as a lawful basis.

6.2 Beyond consent: The remaining exceptions in Article 9

Employers may rely on three further exceptions in Article 9. They are as follows:

(1) Health data may be processed where 'necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment … ' (Article 9 (2)(b));
(2) Health data may be processed where necessary for occupational medicine (Article 9(2)(h)), or
(3) Health data may be processed where necessary for the assessment of the employees' working capacity (Article 9(2)(h)).

These exceptions hinge upon the GDPR's concept of necessity. In order to be lawful, the processing must be necessary in a specific context as laid down in Articles 9(2)(b) and (h).[87] However, the threshold of necessity poses a substantial challenge to employers processing data collected from an employee's fitness tracker as '[e]ssentially, the test for necessity requires a close and substantial connection between the processing and the purposes'.[88] Before delving into the three specific exceptions, we will elaborate upon how necessity is defined in the data protection regime and explain two specific challenges that data controllers face.

6.2[a] *The Necessity Requirement*

The legal concept of necessity was used in the 1995 Directive to delimit the lawful bases[89] and it has an independent EU meaning in the system of data protection.[90] The meaning appears to be consistent between the Directive and the GDPR. An

[86] David Mangan, *Beyond Procedural Protection: Information Technology, Privacy and the Workplace,* 4 EL Rev. 559, 564 (2019).
[87] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Art. 7 of Directive 95/46/EC (2014, WP217), at 13.
[88] Ustaran, *supra* n. 43, at 118.
[89] Article 7 Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

overarching principle of interpretation, as set out consistently by the Court of Justice of the European Union (hereinafter CJEU), is that 'derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary'.[91] From the existing data protection guidance, it appears that the term does not demand that the processing was 'absolutely essential' in the pursuit of the purpose,[92] but the GDPR preamble states that '[p]ersonal data should be processed only if the purpose of the processing could *not reasonably be fulfilled by other means*'.[93]

The amount of data required to achieve the purpose is a matter that the CJEU has shown interest in, ruling that any data processing or sharing beyond what was required to achieve the purpose stated is not legitimate.[94] For example, in *Rīgas satiksme,*[95] the question was whether the police could pass on identifying information about an individual who had damaged the company's property. The CJEU made it clear that, in order to enable the company to sue the wrongdoer, the police could share the address or identification number, as that information would be necessary for the stated purpose.[96] We can thus examine the necessity of data processing in the Wellness and Performance Management models with two issues in mind: (1) could the same aim reasonably be achieved by other, *less privacy-invasive means*? (2) is the *amount and type* of data gathered and processed necessary to achieve the objective or purpose?

With regard to the first issue of whether activity and fitness data processing by an employer is necessary, in light of the other, less privacy-intrusive, means available to achieve the purposes set in a Wellness or Performance Management model, we would make two arguments. First, we question whether it is necessary to share the data gathered by this device with the employer. In a wellbeing-inspired model, for example, a third-party company could be brought in to introduce, supervise and analyse the wearer's data and work directly with registered employees to improve their lifestyle, without sharing data directly with the employer. Secondly, if an employer is considering processing data for performance

---

90 CJEU, *Heinz Huber v. Bundesrepublik Deutschland*, C-524/06, 16 Dec. 2008, ECLI:EU:C:2008:724, para. 52.

91 CJEU, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'*, C-13/16, 4 May 2017, ECLI:EU:C:2017:43, para. 30 and case-law cited therein.

92 Information Commissioner's Office, *Lawful Basis for Processing*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

93 Preamble 39 [emphasis added]. *See also* Ustaran, *supra* n. 43, at 106 and 267; European Data Protection Supervisor (EDPS), *Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (17 Apr. 2017), https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf (especially fn. 14).

94 *Huber*, C-524/06, *supra* n. 90, para. 66; *Rīgas,* C-13/16, *supra* n. 91, para. 30.

95 *Rīgas,* C-13/16, *supra* n. 91, para. 30.

96 Article 9(2)(h) GDPR.

management purposes, one must ask how the data could be considered necessary in pursuit of this objective. The data collected is sensitive; data protection breaches would have potentially serious consequences for employees; and the device itself amounts to a physical intrusion onto the employee's person. Given that traditional performance management mechanisms have been used for many years without incurring these additional privacy and data protection risks, how could an employer argue that activity and fitness monitoring data collection is *necessary* and that performance management cannot reasonably be fulfilled by any other means?

The second challenge in relation to a necessity standard is that of over-collection of data. As demonstrated by the CJEU's consideration of data protection cases, each type of data and the extent of its collection and processing must be necessary to achieve the aim or purpose stated. The difficulty with a wearable device, and the accompanying account, is that it provides *too many categories of information* and, ideally, it tracks the wearer 24 hours a day, seven days a week. If you are an employer seeking to monitor and improve workforce wellbeing, why is it necessary to have the GPS location of your employees at all times? If you are monitoring performance and capability, how would you justify tracking an employee's sleep during annual leave or heart rate on a Saturday night? This difficulty is associated with the adoption of an 'off-the-shelf' solution, in contrast to a data processing scheme using wearable devices to combat an identified health risk associated with the working activities or context.[97]

It is argued that, particularly in combination with the concerns above regarding alternative mechanisms that could achieve the same purpose, employers would struggle to surpass the necessity threshold. Further, the question of necessity must be assessed in relation to the particular aims that are set out in Article 9, as well as demonstrating compliance with the general principle of lawfulness contained in Article 6. In the following two sub-sections, we will consider the Article 9 alternatives in some detail, before briefly discussing Article 6 in the next section.

6.2[b] *Occupational Medicine & Assessment of Working Capacity (Article 9(2)(h))*

Article 9(2)(h) includes a cluster of health-related purposes for which data processing could be considered necessary. Here, we will focus on two of the areas listed

[97] For example, Ibukun Awolusi, Eric Marks & Matthew Hallowell, *Wearable Technology for Personalized Construction Safety Monitoring and Trending: Review of Applicable Devices*, 85 Automation Constr. 96–106 (2018).

in Article 9 that can be applied in the employment context: necessary 'for occupational medicine' and 'for the assessment of the working capacity of the employee'. There is limited EU data protection guidance available on the circumstances in which an employer could rely on these two exceptions.[98] Their application depends entirely on whether either EU or national legislation permits the proposed processing.[99] In addition, the data would have to be processed by a professional under a duty of professional secrecy,[100] such as a doctor or occupational health professional. These preconditions to lawful processing may render reliance on these bases a challenging option for employers, more so once combined with the idea of necessity above.

The 'occupational medicine' exception would not be applicable to employees' health data processing in the Performance Management Model. Here, the purpose of the processing is to monitor employee efficiency and productivity, rather than their health and safety. Whether an employer could rely on this exception to legitimize their data processing in the Wellness Model depends on the scope of the GDPR's definition of 'occupational medicine' and the scope of an employer's duty of care under national occupational health and safety legislations. On the first issue of the definition of 'occupational medicine', there is no European data protection guidance. However, on a literal interpretation of Article 9(2)(h) GDPR, this term could be construed narrowly as relating to measures taken as part of an employer's legal obligation to prevent[101] specific health risks linked to a particular occupation as well as to treat or manage ongoing conditions. Such a definition would exclude monitoring measures that are directed *in a general way* towards changing the lifestyle habits of the workforce. Secondly, the question of whether national occupational health and safety obligations encompass measures to monitor employees' general wellbeing requires further investigation, which is beyond the scope of this article. If the employer satisfies all the requirements under Article 9(2)(h), two Article 6 legal bases could be used: Article 6(1)(c), which permits processing necessary for compliance with legal obligations (health and safety legal obligations in this case) and Article 6(1)(f) which allows processing that is necessary to achieve an employer's legitimate interest (compliance with occupational health and safety obligations in this case).

Turning to 'working capacity', according to the International Association of Privacy Professionals, this may include 'drug testing and other assessments that need to

98 For example, Art. 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final WP 48 (2001), at 16ff. Opinion 2/2017 does not address this topic.

99 *Ibid*.

100 Article 9(3) GDPR.

101 European Parliament, Directorate General for Internal Policies, Study on *Protection of Personal Data in Word-related Relations* 40 (2013).

take place to ensure an employee is fit to work'.[102] This concept is ambiguous and if taken broadly, could encompass concerns about long-term conditions that may develop as a result of a sedentary lifestyle of an employee, for example. When looking at the other areas of activity listed in Article 9(2)(h), however, we observe that the focus appears to be on existing or developing health needs and risks. Whether an employer could use this basis to justify the Wellness Model would depend on national health and safety legislation and the extent to which it permits the monitoring of an employee's general wellbeing as a way to assess his/her fitness to work.[103] Arguably, however, on the basis of a literal interpretation of Article 9(2)(h) GDPR, a *general concern* for employees' well-being as in the Wellness Model will not justify the deployment of a tracking device. Article 6 legal bases will therefore not come into play.

Employers could argue that a Performance Management Model could be used to identify health risks that may undermine an individual's capacity to perform their job effectively, thereby justifying reliance on the 'working capacity' exception. This could be combined with, for example, Article 6(1)(c) (compliance with occupational health and safety legislation) or Article 6(1)(f) (legitimate interest – employees' monitoring for safety and management purpose in this case). We appreciate that, in certain occupations, activity trackers could be useful for such a purpose due to the nature of the job itself. Fitness standards imposed on police officers or military personnel, for example, could be monitored and tracked with the use of a wearable device such as a Fitbit. The same could be said for professions that require a high level of physical and mental fitness such as pilots, train drivers or professional athletes. For example, Crossrail in the UK ran two projects to detect fatigue with the use of wristbands that were able to track and monitor sleep data.[104] There may be challenges related to the other data protection principles, such as data accuracy and minimization, as outlined above. Nonetheless, these occupations in which physical fitness and alertness are critical to one's continued working capacity are an exception where Article 9(2)(h) may be applicable if appropriate implementing measures are in place.[105]

6.2[c] *The Employer's Obligations and Rights in the Field of Employment (Article 9(2)(b))*

[102] Ustaran, *supra* n. 43, at 129.
[103] European Parliament, *supra* n. 101, at 40ff.
[104] Eric Wilson BBA, *Workforce Fatigue Risk Management Using Wearable Technology*, Crossrail Learning Legacy (13 Mar. 2018), https://learninglegacy.crossrail.co.uk/documents/workforce-fatigue-risk-management-using-wearable-technolgy/.
[105] These would include national implementing measures and compliance with the requirement that the processing is overseen by an individual under a professional duty of secrecy.

Beyond the context of the Covid-19 outbreak and its consequences related to data privacy and the processing of the health data of employees,[106] little EU data protection guidance is provided on the extent to which an employer may turn to this exception.[107] The basis in Article 9(2)(b) relies on either EU or Member State law, or a collective agreement, that allows the processing of employee health data. This may encompass legal obligations to ensure health and safety at work, as this is also an area in which Member States can provide more specific rules concerning employee data processing.[108] Given the national character of this exception, it is difficult to evaluate whether an employer will be able to rely on it for the introduction of fitness trackers in line with the Wellness and Performance Management model. The necessity requirement is likely to be a barrier, even if an employer is able to point to national regulations authorizing the data processing that match well the purpose of the two models. If this threshold is surpassed, Article 6(1)(c) and 6(1)(b) would provide two potential routes under Article 6, providing for processing in order to comply with legal obligations (e.g. under occupational health and safety legislation) and for contract performance. Table 2 provides an overview of our analysis in section 6.

Table 2 An Analysis of the Applicability of the Article 9 Exceptions to the Wellness and Performance Management Models

Article 9 Exceptions	*Application of Article 9 Exceptions to the Wellness Model*	*Application of Article 9 Exceptions to the Performance Management Model*	*Potential Article 6 Legal Basis*[109]
CONSENT (Article 9(2)(a))	*Unlikely*: even if explicit, consent not 'freely given' due to presence of imbalance of power (see Article 6(1)(a)).		Article 6(1)(a): consent
OCCUPATIONAL MEDICINE (Article 9(2)(h))	*Unlikely* as definition of 'occupational	*Not applicable* in light of the purpose of monitoring	Article 6(1)(c): compliance with

[106] For example, *German Data Protection Authorities*, https://www.bfdi.bund.de/DE/Datenschutz/Datenschutz-Corona/Allgemeines/FAQ-Corona-Allgemein/Corona-Allgemein_table.html; *see also* Frank Hendrickx, Simon Taes & Mathias Wouters, *Covid-19 and Labour Law in Belgium*, 11(3) Eur. Lab. L.J. 276, 282 (2020) and David Mangan, Elena Gramano & Miriam Kullmann, *An Unprecedented Social Solidarity Stress Test*, 11(3) Eur. L. L.J. 247, 265 (2020).

[107] WP 29, Opinion 8/2001, *supra* n. 98, at 17; Ustaran, *supra* n. 43, at 127.

[108] Article 88 GDPR.

[109] The Article 6 legal bases are only relevant if one of the Article 9 exceptions is applicable. On the applicability of the Article 6 legal bases, *see* section 7 *infra*.

Article 9 Exceptions	*Application of Article 9 Exceptions to the Wellness Model*	*Application of Article 9 Exceptions to the Performance Management Model*	*Potential Article 6 Legal Basis*[109]
CONSENT (Article 9(2)(a))	*Unlikely*: even if explicit, consent not 'freely given' due to presence of imbalance of power (see Article 6(1)(a)).		Article 6(1)(a): consent
OCCUPATIONAL MEDICINE (Article 9(2)(h))	*Unlikely* as definition of 'occupational medicine' in GDPR likely to be narrow. Specificities of national OHS legislation need further examination.	*Not applicable* in light of the purpose of monitoring	Article 6(1)(c): compliance with controller's legal obligations Article 6(1)(f): legitimate interests pursued by the controller

Article 9 Exceptions	*Application of Article 9 Exceptions to the Wellness Model*	*Application of Article 9 Exceptions to the Performance Management Model*	*Potential Article 6 Legal Basis*
ASSESSMENT OF THE WORKING CAPACITY OF A WORKER (Article 9(2)(h))	*Not applicable* in light of the purpose of monitoring	*Possible* only for limited professions due to the nature of the job and subject to the conditions under Article 9(2)(h) and 9(3).	Article 6(1)(c): compliance with controller's legal obligations Article 6(1)(f): legitimate interests pursued by the controller
FULFILMENT OF OBLIGATIONS IN THE FIELD OF EMPLOYMENT LAW (Article 9(2)(b))	*Potentially applicable* but dependent upon European Union/national law/collective agreement authorizing the processing and the presence of appropriate safeguards for data subject's fundamental rights as laid down in national law.		Article 6(1)(c): compliance with legal obligations Article 6(1)(b): performance of a contract

Source: Authors' own elaboration.

7 ARTICLE 6 LEGAL BASES: A FURTHER HURDLE TO LAWFULNESS

If the employer can satisfy the gateway of Article 9's narrow grounds for data processing, they must also demonstrate an Article 6 legitimate basis in order for the processing to be lawful. Here, we focus on two key alternatives: processing necessary for the performance of a contract (Article 6(1)(b)) and processing that is necessary in pursuit of the employer's legitimate interests (Article 6(1)(f)). Consent (Article 6(1)(a)) is not a likely option, as outlined in Section 6.1. A fourth potential basis is Article 6(1)(c), data processing necessary for compliance with a legal obligation to which the controller is subject, which could be relevant to arguments regarding monitoring health and safety risks. This basis however relies heavily on the precise scope of the employer's obligations, which would be determined nationally. These lawful bases invoke the threshold of necessity which was discussed above, and the employer would face additional difficulties in relying on these Article 6 routes to lawfulness which we will outline here.

With regard to contract performance necessity, according to the Working Party, this 'term […] needs to be interpreted strictly' and it cannot be relied upon where the processing is 'not genuinely *necessary* for the performance of a contract, but rather unilaterally imposed on the data subject by the controller'.[110] This condition immediately rules out this legitimate basis for the Performance Management Model, where the data subject only has the stark choice of refusing/leaving the job upon the introduction of a mandatory rule or permitting the processing. Could this basis nevertheless support the Wellbeing Model manner of processing?

We must first identify the central objectives of the relevant contract: the contract of employment. The fundamental objectives of an employment contract are, respectively, to receive the benefit of another's work and to receive the benefit of a wage in return. Employers may therefore use this lawful basis to process the name, contact and financial information of their employees in order *to perform their contractual obligation* to pay employees for their work.[111] From an employee's perspective, however, in most contexts, wearing a tracking device for the collection of health and activity data is *not* necessary for the fulfilment of the contractual obligation to perform work. The only context in which we could foresee this argument may have more success is in the context of occupations, such as athletes, who may be required to track their physical and mental fitness levels in order to

[110] WP 29, Opinion 06/2014, *supra* n. 87, at 16 [emphasis added].
[111] *Ibid.*, at 16. *See also* WP 29, Opinion 2/2017, *supra* n. 67, at 7 and, for the controversial nature of the concept 'contract performance necessity', Mangan, *supra* n. 86, at 565.

perform their central working obligations.[112] Our conclusion here coheres with the analysis provided by Custers and Ursic.[113]

Article 6(1)(f) provides that processing is lawful if it is 'necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject'.[114] There are a number of layers of analysis required here: the identification of a legitimate interest, the necessity requirement, and a balancing between the interest and the interests or fundamental rights of the data subject.[115] At the first stage, it is arguable that 'employee monitoring for safety and management purposes'[116] and 'exercise of [an employer's] rights, such as the right to exercise authority and control'[117] would be considered to be legitimate interests.

We foresee that the most significant challenge for an employer seeking to implement either model is the balancing of its interest with the interests and rights of its employees. Processing device data, as argued in section 2, may amount to an infringement on the employee's fundamental right to privacy, and particularly their privacy with regard to sensitive health data, and it may also have negative consequences for the employee in the future: their autonomy, their reputation and even the possibility of discrimination if a serious health condition is disclosed by the employer's data analysis.[118] All of these rights and interests must be placed in the balance, according to the Working Party.[119] We argue that it would be challenging for an employer to demonstrate that his legitimate interest overrides these rights and interests in implementing fitness trackers in both the Wellness and the Performance Management model.[120]

8 PRIVACY BY DESIGN: A COACHING MODEL TO INTEGRATING FITNESS DEVICES

We have shown that employers opting to store and analyse their employees' data taken from activity tracking devices is unlikely to be compliant with the principle of lawfulness in the GDPR. This argument maintains when examining both the Wellness Model, which is optional and seeks to improve the overall staff health and

112 European Parliament, *supra* n. 101, at 40. *See also* Olsen, *supra* n. 26, at 245.
113 Custers & Ursic, *supra* n. 16, at 334.
114 Article 6(1)(f) GDPR.
115 WP 29, Opinion 06/2014, *supra* n. 87, at 23–24.
116 *Ibid.*, at 25.
117 Hendrickx, *supra* n. 47, at 264.
118 Custers & Ursic, *supra* n. 16, at 324–25 and 342–43.
119 WP 29, Opinion 06/2014, *supra* n. 87, at 37.
120 Custers & Ursic, *supra* n. 16, at 336.

wellbeing, and the Performance Management Model, which would be mandatory. Even in the rare cases that we observed a *potential* route to lawfulness, we have also outlined difficulties in complying with the purpose limitation, data accuracy and data minimization principles in section 4.

Despite these challenges, encouraging employees to live healthy and active lifestyles is sure to benefit both parties to the employment relationship. Even without direct access to the data itself, employers who support the use of activity trackers among their workforce could see benefits in terms of productivity,[121] as well as other effects of a healthier workforce such as lower rates of sick days and health insurance claims. Thus, we might consider how employers *could* lawfully integrate wristband technology into their workplace under the GDPR. Key to the suggestions below are two factors: the *voluntary nature* of the schemes and that *the employer never gains access to the employee's tracking data*.

First, employers may encourage the use of activity trackers and support fitness and mobility within the workplace. Organizations may empower workers to raise issues that they are concerned about with their line manager or occupational health professionals, using the device data as a starting point for the conversation. Such a strategy would not entail the employer processing swathes of metrics from wearable devices and would therefore be respectful of data privacy principles.

An alternative option that is increasingly prominent in the coverage of wellness innovation is the potential of third-party coaching to improve an individual's lifestyle and choices. Some device manufacturers offer this service directly to their customers,[122] though most coaching schemes appear to operate through a specialist coaching company which may use fitness trackers or other wearable health devices to encourage and monitor the wearer's progress towards their health goals.[123] This kind of coaching approach has already been adopted by some companies. For example, BNP Paribas offered employees access to electrocardiogram straps provided by Firstbeat to monitor their heart activity.[124] A physiologist was available to interpret the data and coach the employee based on their personal results. What

[121] Rackspace, *The Human Cloud at Work: A Study into the Impact of Wearable Technologies in the Workplace* (2014), http://smoothmedia.com/project/the-human-cloud-at-work.

[122] For example, Fitbit Care, https://healthsolutions.fitbit.com/healthcoaching/ and Firstbeat Life which aggregates data from their own device, the Firstbeat Bodyguard 3, https://www.firstbeat.com/en/blog/firstbeat-life-faq/.

[123] For example, Firstbeat has a number of local providers in Europe (e.g. Vitality at Work in Belgium) that provide coaching and support to companies in order to manage psychosocial risks such as burnout with the use of the wearable Firstbeat, among others (e.g. *see* https://www.firstbeat.com/en/contact/find-provider/and and https://vitalityatwork.be/mission/).

[124] Katie Scott, *BNP Paribas Uses Wearable Technology to Help Staff Tackle Physical and Mental Stress*, Employee Benefits (23 May 2019, 6 am), https://employeebenefits.co.uk/bnp-paribas-wearable-technology-stress/.

would the responsibilities of the employer and the third-party coaching company be under the GDPR?

The employer, as the party making strategic decisions on the collection of data and its processing, would remain a data controller. The employer would be responsible for ensuring a lawful basis for the processing as well as compliance with all European data protection principles.[125] The third-party company, in conducting the collation, storage and analysis of the data, would be a data processor and therefore also subject to the obligations set out in the GDPR.[126] This is the Regulation's response to an attempt to avoid responsibilities by fragmenting decision-making power across different organizations. It ensures that that all decision-makers and data handlers share the relevant obligations and that a data subject receives protection of their privacy rights regardless of the complexities of the governance structures behind the processing regime.[127]

As the employer is a data controller in relation to the data processing, the range of lawful bases applicable would be limited. Consent would be necessary as a starting point, but in GDPR terms would not provide a legitimate basis for the same reasons outlined above. In order to comply with GDPR, the regime would have to be carefully designed to fit within one of the Article 9 exceptions, possibly occupational medicine (depending on national legislation requirements) or the fulfilment of the employer's obligations in the field of employment. If this threshold of lawfulness could be met, we argue that this alternative is desirable from both an employee and an employer's perspective. The employee's autonomy is protected, their privacy and data protection rights are respected, and the data shared with the employer is minimized. The benefit of a healthier workforce is achieved for the employer, but in a manner that curtails the risks outlined in section 2.

9 CONCLUSION

Employers appear to be endlessly interested in innovative ways to monitor their workers. The huge expansion of the 'data-verse', rapidly developing technology and constantly evolving methods of collecting, combining and analysing data provide new avenues for workforce surveillance. Here, we have unravelled the consequences of an increasingly prominent form of monitoring and emphasized the privacy and autonomy risks that it generates, some of a kind not seen before in the employment context. We argue that employers, in collecting and analysing fitness tracking data, would be processing health data as defined by the Regulation. Without the capacity to rely on

[125] Article 4(7) GDPR.
[126] Article 82 GDPR.
[127] *See*, e.g., Articles 82(2) and 82(4) GDPR.

employee consent to legitimate their processing, we have shown that most employers are likely to struggle to find an alternative lawful basis under Article 9. If the gateway of Article 9 cannot be satisfied, both Wellness and the Performance Management models of implementation would be in breach of the GDPR.

From these arguments, three further points can be contended. First, the conclusions reached here also cast doubt on other, more invasive monitoring practices. Innovations that can closely monitor a worker seem to multiply annually. The Humanyze badge boasts an ability to record forty different types of data about the workers who wear them, including location and quality of interactions with others.[128] The OccupEye monitors precisely when employees are present at their workstation.[129] Microchips can be implanted between the thumb and finger, currently to interact with the environment[130] but with the possibility of tracking capabilities in the future.[131] The companies that develop and implement these apps, packages or devices often rely on the idea of consent: everyone is free to opt in and later to opt out at any time. Our arguments about the validity of an employee's freely given consent undermine these claims, even potentially where the data is processed by a third party.

Secondly, and more generally, we have seen that monitoring must be much more tailored and specific to the purposes pursued by the employer to pass the strict tests of the GDPR. The 'transplantation' of devices from their initial setting (e.g. self-motivation for fitness) to a new context, such as the workplace, poses a serious risk of over-collection of data and raises the possibility of significant privacy, autonomy and data protection breaches for the individual. As our analysis of wristband monitoring shows, a critical evaluation of the lawfulness of each type of data processing by emerging technologies is necessary. Blanket, unthinking, or invasive surveillance is liable to challenge under the GDPR. Overall, we have shown how the GDPR is an important tool in curbing the employer's acquisition of data about their workforce and countering employers' desire for more and more data about their workers.

[128] Ron Miller, *New Firm Combines Wearables and Data to Improve Decision Making*, Tech Crunch (24 Feb. 2015, 5 PM CET), https://techcrunch.com/2015/02/24/new-firm-combines-wearables-and-data-to-improve-decision-making/.

[129] Claire Zillman, *Here's Yet Another Way Your Boss Can Spy on You*, Fortune (13 Jan. 2016, 11:01 PM GMT+1), https://fortune.com/2016/01/13/employee-surveillance-motion-sensors/.

[130] Maggie Astor, *Microchip Implants for Employees? One Company Says Yes*, The New York Time (25 July 2017), https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html.

[131] Jena McGregor, *Some Swedish Workers Are Getting Microchips Implanted in Their Hands*, Washington Post (4 Apr. 2017, 10:40 pm GMT+2), https://www.washingtonpost.com/news/on-leadership/wp/2017/04/04/some-swedish-workers-are-getting-microchips-implanted-in-their-hands/.

These warnings are particularly timely as we write this article during the Covid-19 pandemic. It seems that workers are facing a dramatic acceleration of surveillance, particularly around their health. Both workers who stay at home during periods of self-isolation and employees returning to their workplace face extensive monitoring. Apps such as RescueTime can be used to monitor minute-by-minute productivity while working from home, in the absence of the direct gaze of a supervisor.[132] Away from the home, contact tracing apps pose a clear threat to an individual's privacy and data security,[133] and in the workplace, employers are likely to collect further health data – particularly body temperature – in an attempt to assess whether a worker is showing Covid-19 symptoms.[134] Amazon has built its own Covid-19 testing lab to test samples taken from its employees.[135] Spatial monitoring via wearable trackers and CCTV surveillance are being used to enforce social distancing rules.[136] Although the latter measures could be justified under Article 9(2)(h) due to their connection to the employer's working capacity, they nevertheless amount to an unprecedented invasion into the worker's privacy regarding their health and the implications of a data security breach would be significant.

Thirdly and finally, one way to counteract the imbalance of power existing in an employment relation would be to include workers' voice from an early stage in any decision-making process regarding data processing and employee monitoring. Collective representatives should have input in decisions about how data is collected, as well as how it is processed and analysed by the employer. Scholars have emphasized the significant role that trade unions and other collective organizations could play in the integration of technology throughout work processes.[137] The

---

[132] *See* https://www.rescuetime.com/and on this topic Aiha Nguyen, *On the Clock and at Home: Post-COVID-19 Employee Monitoring in the Workplace*, HR People & Strategy (summer 2020), https://www.hrps.org/resources/people-strategy-journal/summer2020/Pages/feature-nguyen.aspx?utm_source=postcard&utm_medium=directmail&utm_campaign=hrps~2020engagement~nguyensummer2020twitter.

[133] Valerio De Stefano & Christina J. Colclough, *Mind the App*, Bot Populi (23 Apr. 2020), https://botpopuli.net/covid19-corona-contact-tracing-app-human-worker-rights; Aída Ponce Del Castillo, *Covid-19 Contact-tracing Apps: How to Prevent Privacy from Becoming the Next Victim* (ETUI 2020).

[134] See the guidance produced by the UK's ICO for employers, https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/testing/.

[135] BBC News, *Coronavirus: Amazon Builds Its Own Testing Lab for Staff* (10 Apr. 2020), https://www.bbc.co.uk/news/business-35547368.

[136] Synced, *Landing AI 'Social Distancing Detector' Monitors Workplaces*, https://syncedreview.com/2020/04/20/landing-ai-social-distancing-detector-monitors-workplaces/; Rombit, *Smart Bracelet to Prevent Coronavirus Infections on the Workfloor* (17 Apr. 2020), https://rombit.be/smart-bracelet-to-prevent-coronavirus-infections-in-the-workplace/.

[137] Valerio De Stefano, *'Negotiating the Algorithm': Automation, Artificial Intelligence, and Labor Protection*, 41 (1) Comp. Lab. L. Pol'y J. 15, 42ff (2019); Emanuele Dagnino & Ilaria Armaroli, *A Seat at the Table: Negotiating Data Processing in the Workplace: A National Case Study and Comparative Insights*, 41(1) Comp. Lab. L. Pol'y J. 173 (2019).

importance of the collective dimension is also clear from Article 88 GDPR which provides for the possibility of Member States laying down more specific rules for data processing in the employment context through law *or collective agreements*.[138] The European Framework Agreement on Digitalization, adopted in June 2020, represents another major milestone in the adoption of a partnership approach to the implementation of digital technologies in the workplace.[139] This piece has highlighted a number of risks and opportunities which employers, workers and their respective organizations, must take into account in their future negotiations.

[138] Article 88 GDPR.
[139] *European Social Partners Framework Agreement on Digitalization* (June 2020).