



WORKPLACE SURVEILLANCE, HUMAN RIGHTS DUE DILIGENCE, AND PRIVACY BY DESIGN: A CASE STUDY ANALYSIS

Andrijana Bilić, PhD, Full Professor

University of Split, Faculty of Law

Domovinskog rata 8, 21000 Split, Croatia

andrijana.bilic@pravst.hr

ABSTRACT

The rise of surveillance technologies in workplaces has dramatically expanded in recent years. While such technologies promise efficiency gains, they create an atmosphere of “digital panopticism”, thereat posing complex challenges for protecting employees’ privacy. Several complaints have emerged declaring that companies’ algorithmic practices have violated privacy rights and data protection laws. This article critically examines and analyses H&M case, highlighting how failures in Human Rights Due Diligence (HRDD) and Privacy by Design (PbD) have led to significant legal, reputational, and operational risks. Identifying patterns of shortcomings, the author proposes holistic approach, integrating both Human Rights Due Diligence (HRDD) and Privacy by Design (PbD). This approach mitigates the adverse effects of surveillance while prioritizing employee rights, thereby fostering a healthier work environment that enhances mutual trust, respect for employee privacy, and organizational productivity. In the framework of this approach that can create a comprehensive privacy protection system the author proposes best practices for responsible monitoring that respects both human dignity and data protection requirements.

Keywords: Employee privacy protection, H&M case, Human rights due diligence, Privacy by design, Surveillance technologies

1. INTRODUCTION

In the last several decades we have witnessed increased use of digital technologies by the employers in the workplace to monitor their employees, capture and analyse employee data and manage them using algorithms.¹ The revolution in big data

¹ Kellogg, K. C.; Valentine, M. A.; Christin, A., *Algorithms at work: The new contested terrain of control*, Academy of Management Annals, Vol. 14, No. 1, 2020, pp. 366–410; Bailey Diane E, *Emerging tech-*

and artificial intelligence has brought an array of new tools employer use in their business models and methods to control their employees which even have the potential to substantially affect employee's outcome.² The way employers use those technologies, enabling them different types of monitoring,³ is often unclear, not only to employees, but also to policy makers. They are either still operating in the legal vacuum or within legislation that reinforce managerial prerogatives or reflect distrust in employees and indirectly harm them. Some of this harm stem from technology design decision, but more often derive from employers' bad decisions regarding when, why, where and how to use this technology.⁴ Bad decision could, beside the danger of the intrusion into the privacy⁵, lead to other common harms for employees such as: work intensification⁶, health and safety harms⁷, de-skilling⁸,

nologies at work: Policy ideas to address negative consequences for work, employees, and society, ILR Review, Vol. 75, No. 3, 2022, pp. 527–551.

² Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: PublicAffairs, an imprint of Perseus Books, 2019.

³ Types of monitoring companies mostly use are: websites and application usage, time tracking, e mail and Internet monitoring, keystroke logging, screen capture, behavioral analysis and so on.

⁴ Cappelli, P., *Stop overengineering people management*, Harvard Business Review, 2020., September–October. Available at: [https://hbr.org/2020/09/stop-overengineering-people-management], Accessed 8 April 2026.

⁵ Segal, E., *How productivity and surveillance Technology can create a Crisis for Businesses*, Forbes, 18. August 2022; Stanley, J., *The Nightmarish loss of workplace Privacy*, ACLU, 26. August 2022; Roemmich, K.; Schaub, F.; Andalibi, N., *Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy*, Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany. ACM, New York, NY, USA 20 Pages, Available at: [https://doi.org/10.1145/3544548.3580950].

⁶ Schaupp, S., *Cybernetic proletarianization: Spirals of devaluation and conflict in digitalized production*, Capital & Class, Vol. 46, No. 1, pp. 11–31, Available at: [https://doi.org/10.1177/03098168211017614]; Gutelius, B.; Theodore, N., *Technology adoption and the future of warehouse work*, ILR Review 2022., Vol. 75, No. 4, pp. 807–856.; Dzieza, J. *Robots aren't taking our jobs—They're becoming our bosses*, The Verge, February 27. 2020., Accessed 5 February 2025; Carre', E.; Tilly, C., *Digital technology implementation in US retail stores: Trends, potentials, and contingencies*, ILR Review, 2022, Vol. 75, No. 4, pp. 807–856.

⁷ Ravid, D. M. et al., *A meta-analysis of the effects of electronic performance monitoring on work outcomes*. *Personnel Psychology*, 2022, Advance online publication, Available at: [https://doi.org/10.1111/peps.12514]; O'Brady, S.; Doellgast, V., *Collective voice and employee well-being: Union influence on performance monitoring and emotional exhaustion in call centres*, Industrial Relations: A Journal of Economy and Society, Vol. 60, No. 3, 2021, pp. 307–337; Gordon, J.L., *Under pressure: Addressing warehouse productivity quotas and the rise in injuries*, Fordham Urban Law Journal, Vol. 49, No. 1, 2021, pp. 149–189, Available at: [https://link.gale.com/apps/doc/A688295640/AONE?u=irv3447&sid=ebsco&xid=4ac809b7], Accessed 8 April 2026.

⁸ Levy, K.; Solon, B., *Refractive surveillance: Monitoring customers to manage employees*, International Journal of Communication 12, 2018, pp. 1166–1188, Available at: [https://ijoc.org/index.php/ijoc/article/viewFile/7041/2302].

job loss⁹, bias, discrimination¹⁰, suppression of the right to organise¹¹ and loss of autonomy and dignity¹². The extent to which management can now monitor employees' behaviour, both, on-site and remote using advanced surveillance technologies has dramatically increased creating a scenario of panoptic power management (digital panopticism). This phenomenon mirrors Michel Foucault's concept of the "Panopticon"—a structure of control wherein subjects self-regulate under the possibility of constant observation.¹³ In the corporate realm, digital panopticism raises ethical and legal issues around autonomy, privacy, and power asymmetry. Namely, the collection of personal data through various digital means (e.g., emails, productivity software) raises concerns about how this data is stored, used, and shared, potentially causing significant harm to employees' privacy issues and creating the culture of mistrust. Furthermore, organizations may face legal challenges if they fail to comply with privacy regulations leading to financial and repu-

⁹ Kuang-Hsien Wang, K. H.; Lu, W. C., *AI-induced job impact: Complementary or substitution? Empirical insights and sustainable technology considerations*, Sustainable Technology and Entrepreneurship, Vol. 4, Issue 1, 2025; Soueidan, M. H.; Rodwan, S., *The Impact of Artificial Intelligence on Job Loss: Risks for Governments*, Technium Social Sciences Journal, 2024.

¹⁰ Rosenblat, A.; Barocas, S.; Levy, K.; Hwang, T., *Discriminating tastes: Customer ratings as vehicles for bias*, 2016, Data & Society: Intelligence and Autonomy, Available at: [https://datasociety.net/pubs/ia/Discriminating_Tastes_Customer_Ratings_as_Vehicles_for_Bias.pdf], Accessed 8 April 2026.

¹¹ Kessler, S., *Companies are using employee survey data to predict—and squash—union organizing*, One Zero, 30 July 2020, Available at: [https://onezero.medium.com/companies-are-using-employee-survey-data-to-predict-and-squash-union-organizing-a7e28a8c2158], Accessed 29 January 2025.

¹² Groves, K. S.; Margolis, J.; Gibson, C., *Cultivating the experience of dignity at work during digital transformation: Protective & proactive strategies for leaders and organizations*, Organizational Dynamics, 2024.

¹³ Panopticon was elaborated by Jeremy Bentham at the end of the eighteenth century and later on Michel Foucault used it as a symbol of disciplinary power. The simple idea of Bentham can be described as follows: a circular building with the cells of the prisoners located in the circumference and, separated by an empty space, the tower of the inspector located in the centre. The side of each cell facing outwards would be occupied by a large window and the inner one by a thin iron grating in order to make the whole room perfectly visible from the tower, while also contributing to let sunlight inside the Panopticon. The Panopticon is an image for this discipline: in Foucault's opinion its objective is to improve the exercise of power, making it faster, lighter and more effective. The individual in the Panopticon, being subjected to a regime of constant visibility, is caught in a power relationship within which he becomes the principle of his own subjection. Botan, C., *Communication work and electronic surveillance: A model for predicting panoptic effects*. Communication Monographs, 1996., Vol. 63, No. 4, pp. 293–313. [https://doi.org/10.1080/03637759609376396]; Foucault, M., *Panopticism* from "Discipline & Punish: The Birth of the Prison.", Race/Ethnicity: Multidisciplinary Global Contexts, 1996., Vol. 2, No. 1, pp. 1–12, Available at: [http://www.jstor.org/stable/25594995], Accessed 29 January 2026.

tational damages. Although there is established legal framework¹⁴ for the privacy protection, as well as principles derived from ECHR case law¹⁵ the current legal framework has not full potential to resolve conflict of interest between employees' right to privacy and employer's right to protect business interests. This is evident from existing national and European privacy litigations. Bridging this gap requires integration of human rights due diligence (HRDD) and privacy by design (PbD) frameworks into corporate employee privacy system protection which can offer both normative and technical guidance for ethical workplace surveillance.

In the following text, the article examines the publicly documented H&M case through a review of regulatory findings, official reports, academic literature, and secondary legal sources. Rather than presenting an original empirical case study, the article provides a doctrinal and literature-based analysis of a previously reported case in order to identify practical shortcomings in workplace surveillance and employee data protection practices.

The H&M case serves as an illustrative example of how failures in Human Rights Due Diligence (HRDD) and Privacy by Design (PbD) can result in significant legal, reputational, and operational risks for organizations. The purpose of examining this case is not to provide new factual findings or original legal determinations, but rather to identify common patterns of inadequate employee privacy protection and to derive recommendations for improved workplace data governance.

The article further proposes best practices for responsible monitoring that respect both human dignity and data protection requirements. The core objective of this research is to assist employers in incorporating Privacy by Design and Human Rights Due Diligence frameworks into corporate data practices. Beyond constituting a legal obligation, such integration represents a strategic necessity for fostering employee trust and ethical data governance, enabling organizations to build resilient and rights-respecting data ecosystems that safeguard employee dignity in an age of algorithmic management and digital surveillance.

¹⁴ European Convention on Human Rights (1953), the EU Charter of Fundamental Rights (2012), the EU General Data Protection Regulation (GDPR, 2016), EU Directive (EU) 2019/1152, Recommendation CM/Rec (2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment, as well as Opinion 8/2001 on the processing of personal data in the employment context (WP48), the Working Document on the surveillance of electronic communications in the workplace (WP55), and Opinion 2/2017 on data processing at work, ILO Code of Practice on the Protection of Workers' Personal Data (1997).

¹⁵ These principles include: reasonable expectation of privacy; the principle of necessity and proportionality; the principle of legitimacy; the principle of transparency; the principle of finality; the principle of information and consultation.

2. PRIVACY BY DESIGN AT THE WORKPLACE: A PROACTIVE APPROACH TO EMPLOYEE DATA PROTECTION

Implementing Privacy by Design principles in the workplace is essential for safeguarding employee privacy in an increasingly digital environment, building the trust between employers and employees, comply with legal requirements, and mitigate risks associated with data breaches. Privacy by Design is a holistic approach to privacy that encompasses several foundational principles.¹⁶ There are several benefits from incorporating privacy protection into the design of systems and processes from the outset: ensures that risks to employee data are identified and mitigated proactively (e.g., surveillance, productivity tracking, biometric systems); enforces key principles such as data minimization and purpose limitation (e.g., payroll, compliance, safety); fosters transparency and trust within the employment relationship by requiring clear communication about data use and promoting tools such as privacy notices consent mechanisms (where appropriate), and internal data governance policies; due to its alignment with legal obligations laid down in labor laws and fundamental rights protections under EU and international human rights law helps employers regarding lawful processing, fairness, and design-based safeguards; encourage a culture of responsibility and ethical decision-making regarding employee data enhancing organizational accountability; facilitates compliance and promotes ethical, sustainable data practices that protect the fundamental rights of employees.

Design-based approaches are not only popular in the tech industry¹⁷ but have increasingly found their way into legal frameworks¹⁸ and ECHR case law¹⁹. However, several potential shortcomings in design-based approaches have been identified, particularly regarding the adequate protection of privacy in the contemporary workplace:²⁰ struggles to adequately incorporate the principle of proportionality; cannot ex ante balance the competing interests at the moment of decision-making; difficulty to translate ambiguous legal terminology into code;²¹ gaps in

¹⁶ Proactive, not reactive; Preventative, not remedial; Privacy as the default setting; Privacy embedded into design; Full functionality – Positive-sum, not Zero-sum; End-to-end security – Lifecycle protection; Visibility and transparency – Keep it open; Respect for user privacy – Keep it user-centric. See: Cavoukian, A., **Privacy by Design: The 7 Foundational Principles**, Information and Privacy Commissioner of Ontario.

¹⁷ E.g. Microsoft, Apple, Google, IBM, Salesforce, Cisco, Adobe, SAP, Facebook.

¹⁸ Protection by design is an ‘appropriate measure’ to comply with data protection law (GDPR, Art. 25 para. 1).

¹⁹ European Court of Human Rights, *I v. Finland*, App. No. 20511/03, 17 July 2008.

²⁰ More detailed: Ebert, I.; Wildhaber, I.; Adams-Prassl, J., *Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection*, Big Data & Society, Vol. 8 /1, 00, pp. 1-14, p. 5-6.

²¹ Kroener, I.; Wright, D., *A strategy for operationalizing PbD*, The Information Society, Vol. 30, No. 5, 2013, pp. 355–365.

protection are ubiquitous; due to the technological evolution²²; implementation complexity and inconsistent application²³, developing privacy-centric systems can be challenging for smaller organizations due to cost implications; resistance of employees and management to changes especially if they perceive these changes as hindrances to productivity; superficial implementation of privacy measures (PbD approach may sometimes prioritize compliance with legal requirements rather than fostering a culture of privacy within the organization).

In summary, while design-based approaches can enhance employee privacy protection, they also face several challenges. In order to be effective, these approaches must be integrated within broader organizational practices, ongoing training, and a commitment to fostering a culture of privacy. Furthermore, data-driven models that weight human behaviour are not immune to errors or false conclusions about human interaction.²⁴ So, a broader privacy approach is of utmost importance—one that also incorporates ethical expectations by management in decisions about workplace monitoring measures.²⁵ Representatives from all affected stakeholder groups should be strategically involved. All of this brings us to the potential need for the implementation of corporate sustainability due diligence and corporate liability in the legal framework on employee privacy protection.

3. CORPORATE SUSTAINABILITY DUE DILIGENCE AND CORPORATE LIABILITY IN THE EMPLOYEES' PRIVACY PROTECTION

Due diligence' has traditionally been used in national legal frameworks as a standard of care in tort law and comparable concepts in civil law. However, it was not until the last decade that it has emerged as a key mechanism for addressing human rights abuses by businesses. In this context, the notion of prevention is critical, relating to efforts to prevent businesses from causing, contributing to, or being linked to adverse human rights impacts globally.²⁶ HRDD is defined as a compre-

²² Montjoye, Y. *et al.*, *Unique in the crowd: The privacy bounds of human mobility*, 2013, Scientific Reports 3: 1376, Available at: [<https://doi.org/10.1038/srep01376>].

²³ Dix, A., *Built-in privacy— No panacea, but a necessary condition for effective privacy protection*, Identity in the Information Society 3, pp. 257–265.

²⁴ Nagy, P.; Neff, G., *Imagined affordance: Reconstructing a keyword for communication theory*, Social Media & Society 1(2), 2015, Available at: [DOI:10.1177/2056305115603385].

²⁵ Ebert, I.; Wildhaber, I.; Adams-Prassl, J., *Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection*, o. c., p. 6.

²⁶ Human Rights Council, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework: Report of the Special Representative of the

hensive, proactive effort to identify both actual and potential human rights risks over the entire life cycle of a project or business activity, with the aim of avoiding and mitigating those risks^{27, 28}. Integrating HRDD into boardroom decision-making fosters long-term value creation, risk mitigation, and stakeholder trust.²⁹

3.1. Legal framework for corporate sustainability human rights due diligence

While initially introduced as a voluntary standard, HRDD is increasingly being incorporated into binding national legislation³⁰ and supranational regulations. These developments mark a shift toward mandatory HRDD, transforming corporate accountability from a model of soft governance into one of enforceable legal obligations.³¹ At this point, we shall provide an analysis of the non-binding United Nations Guiding Principles on Business and Human Rights, alongside the binding Directive (EU) 2024/1760 (Corporate Sustainability Due Diligence Directive – CSDDD)³².

Although the UNGPs are not legally binding and suffer from weak accountability and enforcement mechanisms³³, inconsistent implementation³⁴, and a limited fo-

Secretary-General on the issue of Human Rights and Transnational Corporations and Other Business Enterprises', UN Doc. A/HRC/17/31, 21 March 2011 ('UNGPs'), Guiding Principle 13.

²⁷ Deva, S., *Regulating corporate human rights violations: Humanizing business*, 2012, Routledge.

²⁸ Human Rights Council, Business and Human Rights: 'Towards Operationalizing the "Protect, Respect and Remedy" Framework', A/HRC/11/13, 22 April 2009, para. 71. See also the UN Working Group on Business and Human Rights, 'The report of the Working Group on the issue of human rights and transnational corporations and other business enterprises', UN Doc. A/73/163, 16 July 2018, para. 10, and OECD, OECD-Due-Diligence Guidance for Responsible Business Conduct (2018), para. 16 ('OECD RBC Guidance').

²⁹ Nolan, J., *The Corporate Responsibility to Respect Human Rights: Soft Law or Not Law?*, in: Backer, L. C. (ed.), Law and Society, 2021, Edward Elgar Publishing.

³⁰ French Duty of Vigilance Law (2017) mandates large companies to implement vigilance plans to prevent human rights and environmental violations and German Supply Chain Due Diligence Act (2021) requires companies to conduct due diligence on human rights and environmental risks across their supply chains.

³¹ Bright, C., et al., *Towards a corporate duty for lead companies to respect human rights in their global value chains?* Business and Politics, Vol. 22, No. 4, 2020, pp. 667–697. Available at: [https://doi.org/10.1017/bap.2020.19].

³² Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859 (Text with EEA relevance), OJ L, 2024/1760, 5 June 2024, *ELI*; Available at: [http://data.europa.eu/eli/dir/2024/1760/oj].

³³ Wettstein, F., *Normativity, Ethics, and the UN Guiding Principles on Business and Human Rights: A Critical Assessment*, Journal of Human Rights, Vol. 14, No. 2, 2015, pp. 162–182.

³⁴ Knudsen, J. S.; Moon, J., *Visible Hands: Government Regulation and International Business Responsibility*, Cambridge Journal of Economics, Vol. 41, No. 2, 2017, pp. 383–409.

cus on power asymmetries³⁵, they are nonetheless regarded as the “global authoritative standard on business and human rights.”³⁶ Their strength lies in their normative clarity and structure³⁷, global legitimacy and endorsement³⁸, its function of catalysing legal and policy reform³⁹ and soft law flexibility⁴⁰. Owing to these strengths, the UNGPs have influenced the incorporation of HRDD into other international standards, national legislation⁴¹, and domestic court decisions⁴². They have also been adopted or referenced by subsequent international instruments.⁴³

Under the CSDDD, member states are obliged to ensure that relevant companies (applies to very large EU companies employing more than 1,000 employees and generating a net worldwide annual turnover of over EUR 450 million, regardless of the sector in which they operate⁴⁴) conduct due diligence⁴⁵. In the context of privacy protection this means that those companies must integrate due diligence into their privacy policies in a way to: identify, prevent, mitigate and end actual or potential adverse impacts on employees’ privacy; on employees’ privacy;

³⁵ Bhatt, R., *Human Rights Due Diligence in Global Supply Chains: Corporate Compliance or Meaningful Accountability?*, Business and Human Rights Journal, Vol. 5, No. 2, 2020, pp. 65–287.

³⁶ International Bar Association, IBA Practical Guide on Business and Human Rights for Business Lawyers, 28 May 2016, Available at: [<https://www.ibanet.org/MediaHandler?id=d6306c84-e2f8-4c82-a86f-93940d6736c4>], Accessed 28 May 2026, p. 13.

³⁷ Ruggie, J. G., *Just Business: Multinational Corporations and Human Rights*, 2013, W. W. Norton & Company.

³⁸ Deva, S.; Bilchitz, D. (eds.), *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect?* Cambridge University Press, 2013.

³⁹ Backer, L. C., *Rights and Accountability in Development: Global Value Chains and Human Rights*, Northwestern Journal of International Law & Business, 2015, 35(3), pp. 387–440; Scheper, C., *From Naming and Shaming to Legal Accountability? The Politics of Human Rights Due Diligence*, Globalizations, 2015, Vol. 18, No. 3., pp. 396–412.

⁴⁰ Kobrin, S. J., *Private Political Authority and Public Responsibility: Transnational Politics, Transnational Firms, and Human Rights*, Business Ethics Quarterly, 2019, Vol. 19, No. 3., 349–374.

⁴¹ These are the French Duty of Vigilance Act 2017 (Devoir de Vigilance Loi), the Dutch Child Labour Due Diligence Act 2019, the German Corporate Due Diligence in Supply Chains Act 2021, Norwegian Transparency Act 2021., Australian Illegal Logging Prohibition Act 2012, the UK Modern Slavery Act 2015 and the Australian Modern Slavery Act 2018.

⁴² Milieudefensie v Royal Dutch Shell, District Court of the Hague, 26 May 2021, ECLI:NL:RB-DHA:2021:5339, available at <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RB-DHA:2021:5339>, especially para. 4.4.11.

⁴³ OECD Guidelines for Multinational Enterprises (2011); the International Labour Organization’s Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy (2017); the International Finance Corporation’s Performance Standards (2012); the 2030 Agenda for Sustainable Development; and most recently, Directive (EU) 2024/1760 (Corporate Sustainability Due Diligence Directive – CSDDD) of the European Parliament and of the Council of 13 June 2024, which also amends Directive (EU) 2019/1937 and Regulation (EU) 2023/2859.

⁴⁴ CSDDD art 2(2).

⁴⁵ CSDDD art. 7.

take ‘appropriate measures’ and take into account specific factors when designing them⁴⁶; establish and maintain a notification and complaints procedure; monitor the effectiveness of their due diligence policy and measures; publicly communicate on due diligence and obligation to conduct meaningful consultation with stakeholders at the different stages of the due diligence process⁴⁷. Stakeholders are widely defined and include companies’ employees, employees of its subsidiaries, trade unions and workers’ representatives, consumers and other affected individuals, groups and communities but also national human rights and environmental institutions or civil society organisations whose purpose includes environmental protection. The CSDDD requires that a company’s due diligence covers not only a company’s operations and the operations of its subsidiaries, but also that of its business partners in its so-called ‘chain of activities’.⁴⁸

The CSDDD is the first mandatory due diligence instrument that introduces two complementary enforcement mechanisms.⁴⁹ The Directive establishes a mixed public and private enforcement regime, involving both public supervisory authorities and a civil liability provision.

As previously noted, due to the limited personal scope of the CSDDD, certain industries and smaller companies are not subject to its obligations and therefore are not required to adopt a human rights due diligence approach to privacy protection in the workplace. In such cases, it becomes essential for companies to adopt internal privacy protection policies that incorporate core data protection principles, such as purpose specification and limitation, prior informed consent, data minimization, use limitation, and, importantly, ethical considerations in order to avoid costly litigation processes. Also, several other shortcomings can be identified with regard to employee privacy protection: lack of specific privacy guidelines,

⁴⁶ CSDDD art. 8.

⁴⁷ CSDDD art 13(3)

⁴⁸ Chain of activities’ means: „activities of a company’s upstream business partners related to the production of goods or the provision of services by that company, including the design, extraction, sourcing, manufacture, transport, storage and supply of raw materials, products or parts of products and the development of the product or the service; and (ii) activities of a company’s downstream business partners related to the distribution, transport and storage of a product of that company, where the business partners carry out those activities for the company or on behalf of the company, and excluding the distribution, transport and storage of a product that is subject to export controls under regulation (EU) 2021/821 or to the export controls relating to weapons, munitions or war materials, once the export of the product is authorised;“ (Art 3(1)(g) CSDDD).

⁴⁹ A 2017 report by the UN Working Group on Business and Human Rights, emphasised the need to ensure that rights holders are an integral part of any process that aims to provide an effective remedy for corporate human rights abuses. UN General Assembly, ‘Report of the Working Group on the issue of Human rights and transnational corporations and other business enterprises’, UN Doc. A/72/162, 18 July 2017.

leading to inconsistent implementation; limited scope, as the Directive may not cover all sectors or types of companies, resulting in regulatory gaps for certain industries and smaller businesses; ambiguity in consent requirements; Insufficient enforcement mechanisms; divergent national interpretations; potential conflicts with other regulations; risk of “tick-box compliance,” whereby companies meet only the minimum legal requirements without meaningfully engaging in due diligence, thereby undermining the Directive’s objectives.

Given that both the *privacy by design* and *human rights due diligence* frameworks exhibit shortcomings in protecting employee privacy, the next section will explore the potential for integrating these two approaches to bridge the existing gaps in this context. As we have seen, although HRDD and PbD share the common goals of protecting privacy and preventing harm, they operate in different yet complementary ways. HRDD offers a broad, human rights-oriented framework that requires companies to actively assess and manage the impact of their actions on workers’ rights. It encourages proactive engagement and stakeholder involvement, which is especially important in workplaces where surveillance and data collection are pervasive. PbD, on the other hand, focuses specifically on data privacy and security at the system level. It requires organizations to embed privacy protections at every stage of data handling—from collection to processing, storage, and destruction. By integrating both approaches, organizations can more effectively safeguard employee privacy, ensuring compliance with legal requirements and adherence to ethical standards in increasingly digitalized workplaces. Real-world examples demonstrate that it is possible to build systems that not only comply with regulations but also uphold fundamental rights.⁵⁰ In the following chapter we shall

⁵⁰ After criticism from privacy advocates and scholars, Microsoft faced scrutiny over its “Productivity Score” tool, initially released as part of Microsoft 365, which allowed employers to monitor individual employee activity. Microsoft revised the tool to align better with human rights and privacy by design principles. The result of the revision is Microsoft’s Productivity Score: Privacy-Centric Redesign, tool that aggregate data at the organizational level, removing identifiable information about individual employees. (The Guardian+2VPN Overview+2Microsoft+2); IBM’s Transparent Remote Work Monitoring- software which IBM implemented during the pandemic for the monitoring of remote workers, which initially faced employee reactions over privacy concerns. In response IBM has incorporated transparent guidelines and employee feedback into the process, demonstrating a commitment to balancing organizational needs with employee privacy. Studies indicate that 54% of employees are more productive when they feel their privacy is respected, Available at: [<https://vorecol.com/blogs/blog-how-do-workplace-surveillance-practices-differ-across-states-and-what-can-employers-learn-from-these-variations-206966?>]; SAP’s SuccessFactors is platform that offers workforce analytics designed with privacy considerations. The system emphasizes data minimization, transparency, and user consent, aligning with privacy by design principles; Cisco’s Ethical Use of Collaboration Analytics - provides analytics tools within its collaboration platforms, such as Webex, to help organizations understand usage patterns. Cisco emphasizes ethical data use by aggregating data and avoiding intrusive monitoring. Their approach includes clear communication with users about

demonstrate how the human rights due diligence and privacy by design failures have created grounds for the employee privacy litigation and company reputational harm. But before we go further it is important to stress that illustrated real-life cases that employers in both cases were not legally bound by CSDDD due to the fact that they took place before Directive came into the force.

3.2. Detailed Case Study: H&M – Covert Employee Profiling

3.2.1. Background⁵¹

H&M Hennes & Mauritz Online Shop A.B. & Co. KG is a fast-fashion chain founded in 1947. and currently headquartered in Stockholm. It currently operates world-wide in 53 online markets and a total of 4,913 stores, with a revenue of 24.25\$ in 2024.⁵²

Hundreds of its employees worked in the Nuremberg Service Centre, and the company retained information about them on their local network drives. In this situation, H&M was both the data controller and the data processor of the employees' (the data subjects) data. Since at least 2014, management at the company collected voice recordings and detailed notes about many employees at meetings called Welcome Back Talks, which occurred after employee absences such as holidays and sick leaves. These consisted of one-on-one conversations between employees and team leaders. These conversations included sensitive health information and vacation experiences, and the related notes included detailed information about the private lives of employees such as family disputes and religious beliefs. Information was processed without the employees' informed consent to create detailed profiles of the employees which were used in their work evaluations. Up to 50 managers throughout the company had at least partial access to this information. In October 2019 the data collected became public knowledge after a configuration error made the data accessible throughout company-wide for a few hours.⁵³ As the service centre is in Nuremberg, it was under the jurisdiction of the

what data is collected and how it is used, ensuring alignment with privacy by design principles (<https://hrtechedge.com/cisco-report-genai-use-raises-employee-privacy-concerns/>).

⁵¹ Taylor, L., *Employee Data Protection and the GDPR: Lessons from the H&M Case*, Journal of Business Ethics, 2021, Vol. 169, No. 2., pp. 291–308, Available at: [<https://doi.org/10.1007/s10551-020-04523-8>].

⁵² Available at: [[http:// https://companiesmarketcap.com/h-m/revenue/](http://https://companiesmarketcap.com/h-m/revenue/)], Accessed 26 March 2026.

⁵³ Available at: [<https://www.cpomagazine.com/data-protection/hm-hit-with-e35-million-gdpr-fine-for-profiling-private-lives-of-employees/>], Accessed 26 March 2026.

HmbBfDI⁵⁴ which was alerted of this privacy violation and, after freezing the network drive, obtaining its 60GB contents, and further investigation, they imposed the €35 million fine against the company a year later.

3.2.2. Human Rights Due Diligence (HRDD) Failures

3.2.2.1. Lack of Impact Assessment

In conducting human rights due diligence business should identify and assess the nature of the actual and potential adverse human rights impacts with which a business enterprise may be involved. This would include: where possible, assessing the human rights context prior to a proposed business activity; identifying potential affected subjects; cataloguing the relevant human rights standards and issues; and projecting how the proposed activity and associated business relationships could have adverse human rights impacts on those identified.⁵⁵ In H&M case there was no conducted privacy impact assessments (PIAs) or HRDD evaluations of its data practices.

3.2.2.2. Absence of Stakeholder Engagement

Business enterprises should seek to understand the concerns of potentially affected stakeholders by consulting them directly in a manner that takes into account language and other potential barriers to effective engagement. This would enable business enterprises to assess their human rights impacts accurately. Where such consultation is not possible, business enterprises should consider reasonable alternatives such as consulting credible, independent expert resources, including human rights defenders and others from civil society.⁵⁶ In H&M case employees were neither informed nor consulted about data collection or surveillance practices, undermining participatory governance.

3.2.2.3. Inadequate Remedy and Non-Judicial Grievance Mechanisms

Where a business enterprise identifies that it has caused or has contributed to an adverse human rights impact through its human rights due diligence process or other means that it has not foreseen or been able to prevent, its responsibility is to require active engagement in remediation, by itself or in cooperation with other actors.⁵⁷

⁵⁴ The Hamburg Commissioner for Data Protection and Freedom of Information.

⁵⁵ UNGP, art. 18 a).

⁵⁶ UNGP, art. 18 b).

⁵⁷ UNGP, art. 22.

To make it possible for grievances to be addressed early and remediated directly, business enterprises should establish effective operational-level grievance mechanisms for individuals and communities who may be adversely impacted. They are typically administered by enterprises, alone or in collaboration with others, including relevant stakeholders. Also, a business enterprise could also participate in the operational-level grievance mechanisms that are provided through recourse to a mutually acceptable external expert or body. Those bringing a complaint do not require first access other means of recourse. They can engage the business enterprise directly in assessing the issues and seeking remediation of any harm. To be effective grievance mechanism should be: legitimate, accessible, predictable, equitable, transparent, rights-compatible and continuous source of learning.⁵⁸

In H&M case there was no grievance mechanisms established prior to exposure, that way violating preventive and remedial standards. Employees were compensated post-facto.

3.2.2.4. Intersection with Privacy-by-Design Principles

The GDPR requirement that requires from the controller, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to protect the rights of data subjects,⁵⁹ also serves as a tool to operationalise HRDD. H&M failed to implement basic privacy-enhancing technologies (PETs), such as pseudonymisation, access restrictions, or retention schedules.

3.2.3. Privacy by Design (PbD) Failures

3.2.3.1. No Lawfulness, Fairness and Transparency'

In collecting personal data, the principles of lawfulness, fairness and transparency' should be respected.⁶⁰ In order for the personal data to be lawfully processed at least one of the following should apply: the data subject has given consent to the processing of his or her personal data for one or more specific purposes; processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a

⁵⁸ UNGP, art.31.

⁵⁹ GDPR, art. 25 (1).

⁶⁰ GDPR, art. 5 (a).

contract; processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; processing 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 which require protection of personal data, in particular where the data subject is a child.⁶¹ Furthermore, GDPR requires that the controller shall take appropriate measures to provide any information regarding personal data processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.⁶²

In H&M case principle of lawfulness was not respected. None of the conditions for the lawfulness of the processing of personal data set in GDPR, art 6, were not met. Also, the principle of transparency was not met due to the fact that the employees were fully unaware of the data collection and its uses.

3.2.3.2. No Purpose Limitation

Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (purpose limitation)⁶³ In the H&M case data was not collected for a specific purpose.

3.2.3.3. No Data Minimisation

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')⁶⁴. In the H&M case the scope of data collected and processed was unjustifiably broad. Namely, collecting health, family, and religious data for routine management decisions exceeded any legitimate necessity.

Furthermore, processing of the personal data must be and is lawful only if at least one of the following applies: the data subject has given consent to the processing

⁶¹ GDPR, art. 6.

⁶² GDPR, art. 12.

⁶³ GDPR, art. 5 (b).

⁶⁴ GDPR, art. 5 c.

of his or her personal data for one or more specific purposes; processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; processing 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 which require protection of personal data, in particular where the data subject is a child.⁶⁵

3.2.3.4. No consent for the Processing of Sensitive Data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (sensitive data) shall be prohibited.⁶⁶ Exceptionally, sensitive data could be processed only if the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent, as well as other justifications listed in GDPR.⁶⁷ Due to the fact that H&M was processing sensitive (health, family, and religious data) it was obliged to proceed in accordance with the conditions for consent set in GDPR.⁶⁸

3.2.3.5. No Security of Processing

Taking into account the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security

⁶⁵ GDPR, art. 6.

⁶⁶ GDPR, art. 9(1).

⁶⁷ GDPR, art. 9.

⁶⁸ GDPR, art. 7.

appropriate to the risk, including inter alia as appropriate: the pseudonymization and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.⁶⁹

In H&M case sensitive data was accessible to a wide group of managers without robust protections, violating GDPR's integrity and confidentiality principles. The discovery of the violation of employee's privacy, was in fact due to a data breach when a configuration error allowed employees throughout the company to view the collected data. The IT specialists at the service centre were responsible for this secondary violation which could have been prevented by violation could have been avoided by more extensive testing and checks on the network configurations.

3.3. Post-Case Developments and Impacts

So, what was the impact of the case on H&M employee's privacy protection? In response to the discovery of these violations, H&M released a press statement taking "full responsibility" for the violation and provided considerable financial compensation to those affected. Furthermore, the company has provided new employee privacy policy to ensure better data protection in the future. Further elements of the newly introduced data protection concept include a newly appointed data protection coordinator, monthly data protection status updates, more strongly communicated whistleblower protection and a consistent information concept.⁷⁰

The H&M case is textbook example of a corporate breakdown in human rights due diligence and PbD failure. It highlights the urgent need for companies to move beyond compliance and adopt holistic, preventative strategies for managing digital risks to employee's privacy. Integrating HRDD with PbD can ensure businesses uphold both regulatory and ethical standards in the datafied workplace. Also, the case demonstrates an increased need for employee education on their data rights and improved whistleblower protections, so that they are able to make violations known.

⁶⁹ GDPR, art. 32.

⁷⁰ Available at: [<https://cs.brown.edu/courses/csci2390/2021/assign/gdpr/lzhu17-h-and-m.pdf>], Accessed 29 March 2026.

4. POLICY RECOMMENDATIONS FOR SAFEGUARDING EMPLOYEE PRIVACY: INTEGRATING HUMAN RIGHTS DUE DILIGENCE AND PRIVACY BY DESIGN IN CORPORATE PRACTICE

Drawing on international human rights standards, legal standards, corporate case studies, and normative frameworks, we have identified key failures in HRDD and privacy by design frameworks in employee privacy settings in real-case scenarios. Now by learning from mistakes we shall outline a best practice scenario for aligning best practice policy recommendations that integrates the principles of Human Rights Due Diligence (HRDD) and Privacy by Design (PbD) frameworks to support employee privacy rights in both regulatory and corporate governance contexts.

To operationalize employee privacy in a rights-respecting and proactive manner, organizations should adopt a policy framework that. The following best practices provide a robust foundation for aligning technological innovation with international human rights standards and data protection norms. A best practice in both Privacy by Design (PbD) and Human Rights Due Diligence (HRDD) is when an organization proactively embeds privacy and human rights considerations into the design, implementation, and governance of its technologies, services, and business operations before harm occurs. In that context companies should apply following HRDD and privacy-by-design principles.

4.1. Policy Recommendations for Corporate Implementation of core HRDD Principles Applied to Employee Privacy

4.1.1. Governance Integration of Employee Privacy

Companies should integrate due diligence policy into their employee privacy and risk management systems,⁷¹ which should be developed in prior consultation with the company's employees and their representatives⁷². Due diligence policy should contain: a description of the company's approach, short-term and long term to due diligence⁷³; a code of conduct⁷⁴ describing rules and principles to be followed throughout the company and its subsidiaries, and the company's direct or indirect business partners and a description of the processes put in place to integrate due diligence into the company's relevant policies and to implement due diligence,⁷⁵

⁷¹ CSDDD, art. 5 1 (a) and art. 7.

⁷² CSDDD, art. 7 (2).

⁷³ CSDDD, art. 7 (2) a.

⁷⁴ CSDDD, art. 7 (2) b.

⁷⁵ CSDDD, art. 7 (2).

including the measures taken to verify compliance with the code of conduct. Companies are obliged to update their due diligence policies without undue delay after a significant change occurs, and review and, where necessary, update such policies at least every 24 months.⁷⁶

4.1.2. Conduct Human Rights Impact Assessments (HRIA) Before Deployment

Organizations must assess the human rights risks of workplace technologies, including surveillance, biometric identification, productivity trackers, and algorithmic management, before deployment. A data protection impact assessment should be carried out prior to implementing an employee monitoring system to weigh up the employer's interests against the risk to employees.⁷⁷ This will help to assess how proportionate and necessary the form of monitoring is and to mitigate the potential risks early. In this context it is of utmost importance to evaluate both actual and potential harms and not just legal non-compliance.⁷⁸

4.1.3. Prevent and Mitigate Adverse Privacy Impacts

Companies must take appropriate measures to identify, prevent, mitigate, or end adverse impacts on employee privacy rights arising from their own operations or those of their subsidiaries and, where related to their chains of activities, those of their business partners. Appropriate measures could include development and implementation of a prevention action plan, with reasonable and clearly defined timelines for the implementation of appropriate measures and qualitative and quantitative indicators for measuring improvement. An action plan may be developed in cooperation with industry or multi-stakeholder initiatives.⁷⁹

4.1.4. Meaningful Stakeholder Engagement

Privacy solutions which include implementation of monitoring or data-driven tools must be co-designed with employees, unions, and ethics committees to reflect diverse workplace experiences (alignment with UNGPs art.18). Participation enhances the legitimacy and effectiveness of workplace monitoring policies and ensures compliance with the UNGPs' requirements for stakeholder engagement. Consultation of stakeholders shall take place at the following stages of the due diligence process: when gathering the necessary information on actual or potential adverse impacts, in order to identify, assess and prioritise adverse impacts; when developing prevention

⁷⁶ CSDDD, art. 7 (3).

⁷⁷ UNGPs art. 17-18.

⁷⁸ CSDDD, art. 8.

⁷⁹ CSDDD, art. 12 (2)a.

and corrective action plans; and developing enhanced prevention and corrective action plans; when deciding to terminate or suspend a business relationship; when adopting appropriate measures to remediate adverse impacts and when developing qualitative and quantitative indicators for the monitoring.⁸⁰

4.1.5. Integration, monitoring and review of privacy safeguards

The companies should embed privacy safeguards into internal processes and governance and continuously assess their effectiveness, especially as technologies and business models evolve. Also, companies should regularly audit surveillance systems and data usage for compliance with rights-based criteria. All these tasks should be at the responsibility of senior management level.

4.1.6. Transparency and justification

Before employee monitoring is implemented, employees (and any agency staff, visitors or other individuals who will be monitored) should be informed about the monitoring and given detailed information including but not limited to information about the nature and extent of the data processing, when and how the data will be obtained, why and how it will be used, who it will be disclosed to, who the data protection officer is, retention periods, the right to lodge a complaint and how confidential or sensitive information will be handled. This should be clearly outlined in accessible workplace privacy notices and relevant internal policies such as 'Acceptable Use/ IT Communications' policies. Regarding the processing of the sensitive data of employees a consumer-focused initiatives like Apple's App Tracking Transparency (ATT) framework which reflects robust privacy-by-design elements should be applied internally to protect employee's privacy. Namely, ATT requires apps to ask users for permission to track their activity across other companies' apps and websites.

4.1.7. Implement Data Minimization and Purpose Limitation

Workplace monitoring should be limited to what is strictly necessary for the specific, legitimate purpose. Regularly audit data processing activities to ensure alignment with stated purposes. Consideration should be given to how to limit the scale and scope of the data obtained (alignment with UNGPs art.13).

If an employer wants to use workplace monitoring to assess employee performance, other less invasive methods which could achieve that aim, should be considered first. Before implementing a close monitoring system, the employer should

⁸⁰ CSDDD, art. 13 (3).

carefully consider will anything new be gained from obtaining more detailed or precise information, or is there already sufficient existing data available. Also, continuous surveillance should be avoided unless justified. Biometric data collection should be limited to legally required or consent-based uses.

4.1.8. Establish Internal Remedy and Accountability Mechanisms

Organizations should provide accessible, confidential, independent and non-retaliatory grievance mechanisms (alignment with UNGPs art.29-31). This is in line with HRDD principle on access to remedy provided in UNGP as well as PbD principle on accountability by design. Features would include anonymous reporting channels, independent oversight bodies (e.g., ethics or compliance boards) and transparent reporting on number and nature of complaints and remediation outcomes. complaints may be submitted by: natural or legal persons who are affected or have reasonable grounds to believe that they might be affected by an adverse impact, and the legitimate representatives of such persons on behalf of them, such as civil society organisations and human rights defenders and trade unions and other workers' representatives representing natural persons working in the chain of activities concerned. The company should provide employees with regular report on privacy grievances and resolutions.⁸¹

4.1.9. Lifecycle Oversight

Privacy and human rights risks are dynamic. Namely, due to a technological shift (e.g., AI, biometric wearables), legal developments (e.g., GDPR, AI Act, CSDDD, ILO conventions) and organizational practices and employee feedback regular audits and evaluations should be institutionalized. In that context companies should carry out periodic assessments of their own operations and measures, those of their subsidiaries and, where related to the chain of activities of the company, those of their business partners, to assess the implementation and to monitor the adequacy and effectiveness of the identification, prevention, mitigation, bringing to an end and minimisation of the extent of adverse impacts. Such assessments shall be based, where appropriate, on qualitative and quantitative indicators and be carried out without undue delay after a significant change occurs, but at least every 12 months and whenever there are reasonable grounds to believe that new risks of the occurrence of those adverse impacts may arise.⁸²

⁸¹ CSDDD, art. 14 (2).

⁸² CSDDD, art. 15.

4.2. Policy Recommendations for Corporate Implementation of Privacy by Design principles under the GDPR

For corporations managing employee privacy in a new complex digital environment, operationalizing these obligations requires a structured, multi-layered approach. The recommendations below represent actionable policies for protecting employee privacy in corporate environments based on GDPR principles.

4.2.1. Integrate Data Protection into the Design of Employment Systems

The company should appoint a data processing officer (DPO) with specific responsibility for employee data protection. It is of utmost importance to ensure independence, adequate resources, and direct reporting lines to senior management. To oversee privacy compliance and integrate privacy risks it is useful to establish a privacy governance committee comprising HR, Legal, IT, Security, and Employee Representatives. Also, it is important to maintain a detailed register of all employee data processing activities, including purposes, categories of data, recipients, legal basis, and retention periods.⁸³ Furthermore, policy framework covering data processing, and employee monitoring protocols should be established.

Companies must implement technical and organizational measures that embed data protection principles, such as⁸⁴, inter alia, minimising the processing of personal data, pseudonymising personal data (for internal analytics to separate identity from behavioral data) as soon as possible, encryption (in particular employee health data and communications, especially when processed remotely or via cloud platforms), transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features directly into the design of employee-related systems (e.g., HR platforms, performance monitoring tools, time-tracking software).⁸⁵

4.2.2. Ensure Data Minimization and Purpose Limitation

The principle of data minimization implies that only data which are adequate, relevant and limited to what is necessary in relation to the specified, explicit and legitimate purposes for which they are processed and not further processed in a manner that is incompatible with explicit purposes should be processed.⁸⁶ That obligation applies to the amount of personal data collected, the extent of their

⁸³ GDPR, art.30.

⁸⁴ GDPR, recital 78.

⁸⁵ GDPR, art. 25 (1).

⁸⁶ GDPR, art. 5 (1) a, b, c.

processing, the period of their storage and their accessibility. In line with this, companies should avoid pervasive surveillance (e.g., keystroke logging, location tracking), unless demonstrably necessary. Also, it is important for the company to define narrowly tailored purposes for each type of employee data and document the legal basis for lawful processing.

4.2.3. Role-Based Access Controls and Internal Data Governance

Companies should employ access restrictions to ensure that only by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons, but to personnel who need employee data to perform their job functions have access to it.⁸⁷ With that purpose companies should implement role-based access controls and regularly review access logs. The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.⁸⁸

4.2.4. Conduct Data Protection Impact Assessments for High-Risk Processing

Where a type of processing in particular using new technologies as often occurs in workplace surveillance or algorithmic management, is likely to result in a high risk to employee privacy protection, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. The controller could seek the advice of the data protection officer, employee representatives, and IT security experts where designated, when carrying out a data protection impact assessment. A data protection impact assessment shall in particular be required in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.⁸⁹ A data protection impact assessment should follow next steps:

- state the purpose of processing and describe the processing procedure;
- respect the principle of necessity and proportionality,
- identify risks to employee's rights and freedoms;
- define mitigation measures;
- consult employee representatives and data processing officer;

⁸⁷ GDPR, art. 25(2).

⁸⁸ GDPR, art. 32 (1) b.

⁸⁹ GDPR, art. 35 (3) a and recital 91.

- document outcomes and integrate into project risk management.

4.2.5. Implement Transparency and Employee Rights Awareness Measures

When processing employee's data the company (the controller) should take appropriate measures to provide any information referred to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.⁹⁰ Transparent processing is a prerequisite for fair and lawful data processing. Privacy by Design requires that employees understand what data is collected, why, and how it is protected. With a purpose of raising employee's awareness of their rights to privacy protection the access to self-service portals should be enabled. The self-service portals enable employees to:

- view collected data;
- correct inaccuracies;
- exercise data portability;
- withdraw consent;
- object to specific processing

5. CONCLUSION

In the digital economy, employee privacy has become a frontline issue. Companies that collect and process great amounts of employee's personal data must strike a right balance between operational efficiency and employee privacy and well-being. As corporate data ethics evolve, applying privacy by design and human rights due diligence across all data subjects, employees included, must become standard practice. Companies should harmonize their external privacy leadership (customer privacy) with their internal governance systems (employee privacy). Applying the same ethical and legal standards to employee data as to consumer data is not only a compliance requirement but a strategic imperative in the age of responsible innovation and AI governance. Responsible monitoring regime choices combined with strong data governance policies can allow businesses to responsibly collect and process employee's data. Fostering a culture of mutual trust while protecting stakeholder interests is critical as virtual and hybrid work persists. The most effective approach to operationalize employee privacy in a rights-respecting and proactive

⁹⁰ GDPR, art. 12 (1).

manner is for organizations to adopt a policy framework that integrates the principles of Human Rights Due Diligence (HRDD) and Privacy by Design (PbD).

REFERENCES

BOOKS AND ARTICLES

1. Backer, L. C., *Rights and Accountability in Development: Global Value Chains and Human Rights*, Northwestern Journal of International Law & Business, 35, No. 3, 2015, pp. 387–440
2. Bailey, Dieane E., “*Emerging Technologies at Work: Policy Ideas to Address Negative Consequences for Work, Employees, and Society.*”, ILR Review 75, No. 3, 2022, pp. 527–551
3. Bhatt, R., *Human Rights Due Diligence in Global Supply Chains: Corporate Compliance or Meaningful Accountability?*, Business and Human Rights Journal 5, No. 2, 2020, pp. 265–287
4. Botan, C., *Communication work and electronic surveillance: A model for predicting panoptic effects*, Communication Monographs 63, No. 4, 1996, pp. 293–313, Available at: [<https://doi.org/10.1080/03637759609376396>]
5. Bright, C.; Marx, A.; Pineau, N.; Wouters, J.; Wright, J., Towards a corporate duty for lead companies to respect human rights in their global value chains? *Business and Politics* 22, No. 4, 2020, pp. 667–697
6. Cappelli, P., *Stop overengineering people management*, Harvard Business Review, 2020., September–October, Available at: [<https://hbr.org/2020/09/stop-overengineering-people-management>]
7. Carre', F.; Tilly, C., *Digital technology implementation in US retail stores: Trends, potentials, and contingencies*, ILR Review 75, No. 4, 2022, pp. 807–56
8. Deva, S., *Regulating corporate human rights violations: Humanizing business*, Routledge, 2012
9. Deva, S.; Bilchitz, D. (eds.) *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect?*, Cambridge: Cambridge University Press, 2013
10. Dix, A., “*Built-in Privacy - No Panacea, but a Necessary Condition for Effective Privacy Protection.*” *Identity in the Information Society* 3, 2010, pp. 257–265
11. Ebert, I.; Wildhaber, I.; Adams-Prassl, J., *Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection*, Big Data & Society 8, No. 1, 00, 2021, pp. 1–14
12. Groves, K. S.; Margolis, J.; Gibson, C., *Cultivating the experience of dignity at work during digital transformation: Protective & proactive strategies for leaders and organizations*, Organizational Dynamics, 2024
13. Gutelius, B.; Theodore, N., *Technology adoption and the future of warehouse work*, ILR Review 2022, Vol. 75, No. 4, pp. 807–856
14. Kellogg, K., C.; Valentine, M. A.; Christin, A., *Algorithms at work: The new contested terrain of control*, Academy of Management Annals, Vol. 14, No. 1, 2020, pp. 366–410
15. Kessler, S., *Companies are using employee survey data to predict—and squash—union organizing*, One Zero, 2020, July 30, Available at:

- [<https://onezero.medium.com/companies-are-using-employee-survey-data-to-predict-and-squash-union-organizing-a7e28a8c215>], Accessed 6 January 2025
16. Knudsen, J. S.; Moon, J., *Visible Hands: Government Regulation and International Business Responsibility*, Cambridge Journal of Economics, Vol. 41, No. 2, 2017, pp. 383–409
 17. Kobrin, S. J., *Private Political Authority and Public Responsibility: Transnational Politics, Transnational Firms, and Human Rights*, Business Ethics Quarterly, Vol. 19, No. 3, 2019., pp. 349–374
 18. Kroener, I.; Wright, D., *A strategy for operationalizing PbD*, The Information Society, 2014, Vol. 30, No. 5, pp. 355–365
 19. Kuang-Hsien Wang, K. H.; Lu, W. C., *AI-induced job impact: Complementary or substitution? Empirical insights and sustainable technology considerations*, Sustainable Technology and Entrepreneurship, Volume 4, Issue 1, 2025
 20. Levy, K.; Solon, B., 2018., Refractive surveillance: Monitoring customers to manage employees. International Journal of Communication, 2018, 12, pp. 1166–1188, Available at: [<https://ijoc.org/index.php/ijoc/article/viewFile/7041/2302>]
 21. Montjoye, Y., *et al.*, *Unique in the crowd: The privacy bounds of human mobility*, Scientific Reports 3: 1376, 2013, Available at: [<https://doi.org/10.1038/srep01376>]
 22. Nagy,P.; Neff, G., *Imagined affordance: Reconstructing a keyword for communication theory*, Social MediaSociety1(2), 2015, Available at: [DOI:10.1177/2056305115603385]
 23. Nolan, J., *The Corporate Responsibility to Respect Human Rights: Soft Law or Not Law?*, in: L. C. Backer (ed.), Law and Society, Edward Elgar Publishing, 2021
 24. O’Brady, S.; Doellgast, V., *Collective voice and employee well-being: Union influence on performance monitoring and emotional exhaustion in call centres*, Industrial Relations: A Journal of Economy and Society, Vol. 60, No. 3, 2021, pp. 307–337
 25. Gordon, J.L., *Under pressure: Addressing warehouse productivity quotas and the rise in injuries*, Fordham Urban Law Journal, Vol. 49, No. 1, 2021, pp. 149–189, Available at: [<https://link.gale.com/apps/doc/A688295640/AONE?u=irv3447&sid=ebsco&xid=4ac809b7>]
 26. Ravid, D. M. *et al.*, *A meta-analysis of the effects of electronic performance monitoring on work outcomes*, Personnel Psychology, 2022, Advance online publication, Available at: [<https://doi.org/10.1111/peps.12514>]
 27. Roemmich, K.; Schaub, F.; Andalibi, N., *Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy*, in: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI ‘23), April 23–28, 2023, Hamburg, Germany. ACM, New York, NY, USA 20 Pages, Available at: [<https://doi.org/10.1145/3544548.3580950>]
 28. Rosenblat, A.; Barocas, S.; Levy, K.; Hwang., T., *Discriminating tastes: Customer ratings as vehicles for bias*. *Data & Society: Intelligence and Autonomy*, 2016, Available at: [https://datasociety.net/pubs/ia/Discriminating_Tastes_Customer_Ratings_as_Vehicles_for_Bias.pdf]
 29. Ruggie, J. G., *Just Business: Multinational Corporations and Human Rights*, W. W. Norton & Company, 2013

30. Schaupp, S., *Cybernetic proletarianization: Spirals of devaluation and conflict in digitalized production*, Capital & Class, Vol. 46, No. 1, pp. 11–31. Available at: [\[https://doi.org/10.1177/030981682111017614\]](https://doi.org/10.1177/030981682111017614)
31. Scheper, C., *From Naming and Shaming to Legal Accountability? The Politics of Human Rights Due Diligence*, Globalizations, Vol. 18, No. 3, 2018, pp. 396–412
32. Segal, E., *How productivity and surveillance Technology can create a Crisis for Businesses*, Forbes, 18 August 2022
33. Soueidan, M., H.; Rodwan, S., *The Impact of Artificial Intelligence on Job Loss: Risks for Governments*, Technium Social Sciences Journal, 2024
34. Stanley, J., *The Nightmarish loss of workplace Privacy*, ACLU, 26. August 2022
35. Taylor, L., *Employee Data Protection and the GDPR: Lessons from the H&M Case*. Journal of Business Ethics, Vol. 169, No. 2, 2021, pp. 291–308, Available at: [\[https://doi.org/10.1007/s10551-020-04523-8\]](https://doi.org/10.1007/s10551-020-04523-8)
36. Wettstein, F., *Normativity, Ethics, and the UN Guiding Principles on Business and Human Rights: A Critical Assessment*, Journal of Human Rights, Vol. 14, No. 2, 2015, pp. 162–182
37. Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: PublicAffairs, an imprint of Perseus Books, 2019

EU LAW AND LEGAL DOCUMENTS

1. Directive (EU) 2024/1760 (Corporate Sustainability Due Diligence Directive – CSDDD) of the European Parliament and of the Council of 13 June 2024, which also amends Directive (EU) 2019/1937 and Regulation (EU) 2023/2859
2. Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937
3. EU Charter of Fundamental Rights (2012)
4. EU Directive (EU) 2019/1152
5. EU General Data Protection Regulation (GDPR, 2016)
6. European Convention on Human Rights (1953)
7. French Duty of Vigilance Act 2017 (Devoir de Vigilance Loi)
8. Human Rights Council, ‘Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework: Report of the Special Representative of the Secretary-General on the issue of Human Rights and Transnational Corporations and Other Business Enterprises’, UN Doc. A/HRC/17/31, 21 March 2011 (‘UNGPs’), Guiding Principle 13
9. Human Rights Council, Business and Human Rights: ‘Towards Operationalizing the “Protect, Respect and Remedy” Framework’, A/HRC/11/13, 22 April 2009
10. ILO Code of Practice on the Protection of Workers’ Personal Data (1997)
11. International Bar Association, *IBA Practical Guide on Business and Human Rights for Business Lawyers*, 28 May 2016, Available at: [\[https://www.ibanet.org/MediaHandler?id=d6306c84-e2f8-4c82-a86f-93940d6736c4\]](https://www.ibanet.org/MediaHandler?id=d6306c84-e2f8-4c82-a86f-93940d6736c4)
12. International Finance Corporation’s Performance Standards (2012)

13. International Labour Organization's Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy (2017)
14. Norwegian Transparency Act 2021
15. OECD Guidelines for Multinational Enterprises (2011)
16. Opinion 2/2017 on data processing at work
17. Opinion 8/2001 on the processing of personal data in the employment context (WP48),
18. Recommendation CM/Rec (2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment
19. Regulation (EU) 2023/2859 (Text with EEA relevance), OJ L, 2024/1760, 5.7.2024, ELI
20. The 2030 Agenda for Sustainable Development; and most recently
21. The Dutch Child Labour Due Diligence Act 2019
22. The German Corporate Due Diligence in Supply Chains Act 2021
23. UK Modern Slavery Act 2015
24. UN General Assembly, 'Report of the Working Group on the issue of Human rights and transnational corporations and other business enterprises', UN Doc. A/72/162, 18 July 2017
25. UN Working Group on Business and Human Rights, 'The report of the Working Group on the issue of human rights and transnational corporations and other business enterprises', UN Doc. A/73/163, 16 July 2018, para. 10, and OECD, OECD-Due-Diligence Guidance for Responsible Business Conduct (2018), para. 16 ('OECD RBC Guidance')
26. Working Document on the surveillance of electronic communications in the workplace (WP55)

EUROPEAN COURT OF HUMAN RIGHTS

1. European Court of Human Rights, *I v. Finland*, App. No. 20511/03, 17 July 2008
2. *Milieudefensie v Royal Dutch Shell*, District Court of the Hague, 26 May 2021, ECLI:NL:RBDHA:2021:5339

WEBSITE REFERENCES

1. Cavoukian, A., "*Privacy by Design: The 7 Foundational Principles, 2010.*", Information and Privacy Commissioner of Ontario, Available at: [<https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>]. Accessed 20 May 2025
2. Foucault, M., "*Panopticism*" from "*Discipline & Punish: The Birth of the Prison.*", Race/Ethnicity: Multidisciplinary Global Contexts, Autumn, 2008, Vol. 2, No. 1, The Dynamics of Race and Incarceration: Social Integration, Social Welfare, and Social Control, *Indiana University Press* 2, no. 1, 2008, pp. 1-12, Available at: [<https://web.colby.edu/pl422-spring22/files/2022/01/Foucault-Panopticism.pdf>], Accessed 10 February 2025