Vol. 08, No. 1 (2026) 189-196, doi: 10.24874/PES08.01.020

Proceedings on Engineering Sciences

www.pesjournal.net

SYNERGY BETWEEN INDUSTRY 4.0 AND PERSONAL DATA PROTECTION: LEGAL CHALLENGES AND COMPLIANCE STRATEGIES

Drissi Imane [1]
Mohammed Chakib Himmich

Received 10.07.2025.
Revised 27.10.2025.
Accepted 07.11.2025.

Keywords:

Industry 4.0, Personal data, Data protection, Compliance strategies, International standards, GRPD, Digital boundaries

A B S T R A C T

The rise of digital technologies is driving a profound transformation in our society, affecting not only the way we communicate but also our lifestyles, work habits, and social interactions. Industry 4.0, which integrates smart technologies into production processes, represents the current industrial revolution, characterized by the digital interconnection of machines. However, this evolution raises significant challenges in terms of personal data protection, which lies at the heart of this digital transformation. The global flow of data, facilitated by the Internet and cyberspace, challenges traditional legal boundaries of protection. This work aims to examine the synergy between Industry 4.0 and personal data protection by analyzing the legal issues and international compliance strategies needed for better optimization of privacy in the digital age.

1. INTRODUCTION

Our society is undergoing a profound transformation as a result of digital technologies. It's not just the way we communicate that's changing, but also the way we live, work and interact in society.

Digital infrastructure and data management are two of the key factors associated with digitalization. As a result, the way we consume is changing, as are our needs and expectations for protection and security (Féral-Schuhl, 2019).

The digital transformation has profoundly changed the economy and society to the extent that almost all productive activities will have a digital dimension. At the heart of this transformation is Industry 4.0: production in which all machines communicate with each other digitally (Julien & Martin, 2021).

Industry 4.0 can be defined as the integration of intelligent digital technologies into production and industrial processes (Feillens, 2024).

A new generation of connected, smart factories. Industry 4.0 is the latest of the three industrial revolutions. It's called that because the innovation behind these industrial revolutions didn't just marginally improve productivity and efficiency: it completely revolutionized production and the organization of work.

The invention of the steam engine led to the first industrial revolution in the 19th century. Mass production, embodied by Fordism and Taylorism,

[1] Corresponding author: Drissi Imane
Email: imane.drissi2@uit.ac.ma

changed the face of industry forever in the early 20th century.

Then, starting in the 1960s, it was the turn of robotics and industrial computing to provide unprecedented technical resources.

Since 2000, we've been experiencing the Fourth Industrial Revolution. Technically, it is the hybridization of the automated and computerized factories of the first three industrial waves with the information technologies of the Internet age.

Driven by new information and communication technologies (NICT), this new industrial sector is helping to lower the boundaries between the physical and digital worlds and represents a true revolution in the industrial sector (Hilary & Serret, 2024).

At the heart of the new Industry 4.0 is personal data. Its global circulation calls into question the notion of borders, which is the foundation of the era to which the law applies.

The development of the Internet has led to the creation of a cyberspace in which data circulate freely, free of state borders. This technological revolution raises important questions about the protection of personal data, particularly in view of the increase in the collection, processing and storage of sensitive data.

The implementation of Industry 4.0 requires special attention to the legal requirements related to data protection, as well as the adoption of compliance strategies adapted to European standards, in particular the General Data Protection Regulation.

Semantically, the aim of this article is to analyze the synergy between Industry 4.0 and the legal protection of personal data, by creating a concordance table between the principles of the industry of the future and data protection obligations.

In this sense, it was imperative for us to provide an answer to the following problem, from a purely legal prism: How can Industry 4.0, between the increased use of digital technologies and massive data collection, be in synergy with the legal protection of personal data?

Faced with the same need to strengthen the legal framework for the protection of personal data, we thought it appropriate to divide our study into two parts: the first examines this need in light of the requirements of Industry 4.0, while the second analyzes the implementation of the obligations of those responsible for smart factories.

2. THE NEED TO STRENGTHEN THE LEGAL FRAMEWORK FOR DATA PROTECTION TO MEET THE CHALLENGES OF INDUSTRY 4.0

Fully globalized, instantaneous exchange systems based on increasingly powerful digital technologies are challenging the land and sea borders of states due to the speed of data circulation in an invisible, borderless space. It goes without saying that securing data is an essential link in the success of any digital project, especially Industry 4.0, an industry that holds technological promise but faces legal challenges related to the massive collection of personal data.

2.1 The challenges of massive data collection and management

The advent of Industry 4.0 represents a major digital transformation, in which automated data collection has become a central pillar (Collin-Lachaud, 2022).

This revolution is fueled by a multitude of Internet of Things (IoT) sensors and systems that provide massive amounts of data in real time. This includes information that can be linked to individuals, such as biometrics, consumer habits or online behavior.

Once collected, this data is the essential raw material for production process optimization and predictive maintenance. However, this massive collection poses privacy and data security risks. Information capital is often underutilized, but it deserves to be identified and protected (Julien & Martin, 2021).

The collection and processing of personal data in industry presents a number of significant challenges, not least because of the sensitive nature of the information and the strict legal requirements for its protection. In today's environment, it is essential to ensure the integrity, confidentiality, availability and traceability of personal data (Féral-Schuhl, 2019). This plays a fundamental role in the security of information systems, the protection of individual privacy and compliance with current regulations, such as the General Data Protection Regulation (GDPR) in Europe.

2.2 Ethical practices in personal data collection

The scale of data collection and sharing has increased dramatically (Table 1). Technologies are enabling smart industry to use personal data as never before in its activities (Féral-Schuhl, 2019).

And it is often not possible to fully identify the purpose of the processing of personal data for industrial activities at the time of massive data collection.

Therefore, data subjects should be able to give their consent to the collection of their personal data in the context of their professional activities in the Smart Factory, as far as the intended purpose allows.

As highlighted in Recital 4 of the GDPR: "The processing of personal data should be designed to serve humanity ... in accordance with the principle of proportionality". Indeed, the right to the protection of personal data must be reconciled with other fundamental rights, such as freedom of expression or the right to public security. This recital is in line with the principle of proportionality, which requires that any restriction of a fundamental right, including the right to the protection of personal data, must be necessary, proportionate and appropriate to the objective pursued (Reis & Melão, 2023).

In an environment increasingly focused on automation and digitization, by respecting this principle of proportionality, smart factories will not only be able to comply with European legal requirements, but will also adopt an ethical stance that protects the rights of individuals and fosters trust in technology (Julien & Martin, 2021).

Table 1. Ethical framework applicable to the practices of collecting and using personal data.

Ethical Perspectives	Definitions	Applications to data collection and usage practices
Virtue Ethics	Involves observing a person (or a company) and the appropriate character of their actions, considering both the intended and unintended effects of their actions on others (Herschel & Miori, 2017).	Necessity to identify the intentions (or purposes) of the concerned entity and assess their value for consumers. Understanding the conditions of data usage (e.g., data collected, exchanged, recalculated) to evaluate the intended and unintended effects (i.e., risks) of actions on consumers.
Social Contract Theory	The moral obligations of individuals (or a company) depend on a contract or agreement between them and society (Donaldson & Dunfee, 1999).	Evaluate the implicit norms, based on the context and types of data used: (1) whether the data should be accessed by third parties, and (2) the objectives of these usages (Martin, 2016).
Kantian Ethics	Argues that one must always respect the autonomy and rationality of others, treating them as ends in themselves and never merely as means to achieve an end (Herschel & Miori, 2017).	Evaluate the degree of preservation of autonomy and rationality of individuals through data use: - Level of awareness of individuals about how their data is used. - Level of consent provided by individuals for these practices.

It is this ethics of personal data collection practices that will ensure that Industry 4.0 does not become a sphere where data exploitation is at the expense of individual freedoms and fundamental values.

In other words, the collection of personal data in Industry 4.0 must be guided by a strict ethical framework in which respect for human dignity, transparency and purpose limitation are imperatives (Blanchet, 2022a)

3. COMPLIANCE WITH THE PURPOSE LIMITATION PRINCIPLE

The collection of personal data must be designed to respect the general interest (in the service of humanity), but in compliance with specified and legitimate purposes. Article 5 (1.b) of the RGPD stipulates that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes ...".

More specifically, when personal data is collected, the purpose of the data processing must be clear and transparent. The data must be processed only to achieve the stated purpose. For example, if a company collects information to register for a service, it cannot use the same data to send advertising without the explicit consent of the individual.

In Industry 4.0, the data collected can also be used to optimize machine performance, predict breakdowns, adjust production in real time, or improve logistics processes thanks to AI algorithms.

The purpose of this data collection must be clearly defined and communicated to employees and all stakeholders, as this principle is part of the security of the data collected.

3.1 Challenges in securing the data collected

Securing personal data is a critical issue that aims to maintain the confidentiality, integrity, and availability of information through the application of information security processes (Bensoussan et al., 2016).

In today's context of ubiquitous data collection and processing, the challenges of securing personal data in the context of Industry 4.0 are numerous and complex. The industry of the future, characterized by the integration of advanced technologies (IoT, AI, connected sensors ...), poses particular challenges in terms of securing personal data (Arroyo et al., 2018).).

These technologies are transforming industrial and commercial processes, but they are also increasing the risks associated with legally securing personal data.

3.2 Managing Sensitive Data

Industry 4.0 technologies generate and collect massive amounts of personal data, especially through sensors and connected devices. This data can include information about employees (biometrics, location) or customers (preferences, purchasing behavior) (Ngombé, 2024). With security measures adapted to the nature of this information and the risks it poses. The challenge for Industry 4.0 is to ensure that this sensitive data is processed in accordance with European Union legislation, in particular the GDPR, in which Recital 51 states: "Personal data which, by their nature, are particularly sensitive from the point of view of fundamental rights and freedoms, deserve special protection because the context in which they are processed could give rise to significant risks for those rights and freedoms".

Since the beginning of the Covid-19 crisis, attacks against companies worldwide have multiplied, in particular through phishing campaigns that take advantage of public fears and the insecure nature of certain connections, such as mobile devices (CNIL, n.d.)

The opening up of industrial control systems to the Internet also raises the question of their resistance to computer viruses, whether deliberately introduced or not, which can affect the operation of the equipment and, consequently, the protection of the employee data collected. This makes cybersecurity a major challenge to protect both data and equipment (Julien & Martin, 2021).

Ensuring integrity, confidentiality, availability, and traceability, especially for critical systems, has become a major challenge for both productivity and maintaining customer and partner confidence.

Preventing computer incidents and attacks is often a matter of simple reflexes that contribute to the overall protection of the smart factory.

3.3 Cloud data protection

Cloud security is a set of practices and technologies designed to address external and internal threats to the security of enterprises that need to secure the cloud as they implement their digital transformation strategy and integrate cloud-based tools and services into their infrastructure (Plouin, 2022).

In an ever-changing environment such as Industry 4.0, it's important to automate security processes to quickly respond to threats and ensure real-time compliance.

Smart factories use cloud solutions to store and process data at scale. These cloud services can involve international data transfers, raising important security and RGPD compliance issues.

To manage a cohesive hybrid and multi-cloud security program, it is essential to establish visibility and control that can help orchestrate workload deployment and establish effective threat prevention (Schaeffer, 2017).

The challenge, then, is to ensure the security of data stored in the cloud while complying with international data transfer regulations (in particular, Articles 44 through 50 of the RGPD) and holding those responsible for factories 4.0 accountable.

Moving to the cloud is a bit like bringing electricity to factories. Always with the goal of improving data security. It's a move that can dramatically reduce the size of your entire IT infrastructure and provide better security, especially as your infrastructure ages (Blanchet, (2022b).

4. STRENGTHENING THE LEGAL FRAMEWORK BY DEFINING THE OBLIGATIONS OF MANAGERS

Factory 4.0 offers many new opportunities, all of which are closely linked to data processing as part of the management of employees, customers or even users of industrial products.

And to ensure the secure management of the data collected by the factory of the future, it is essential to review the robustness of the regulatory framework.

This approach aims to reconcile technological innovation with the protection of personal data, while complying with global standards and regulations. One of the first steps in this reconciliation is to comply with the EU's GDPR, a globally recognized model that imposes strict obligations on the processing of personal data.

As such, smart factories need to incorporate these regulations into their processes from the design stage of their systems. This includes liability obligations related to the processing of personal data, especially when international transfers are involved.

4.1 Responsibility for data processing

In order to comply with European standards, particularly in the area of personal data protection, Factories 4.0 must be technologically mature, which implies strict obligations in terms of responsibility and transparency. Genuine protection of personal data in Factories 4.0 requires not only a strengthening of the rights of individuals, but also a clarification of the responsibilities associated with the processing of personal data.

As a result, smart factories must ensure that data collected is accurate, secure, and deleted when no longer needed. Conversely, Recital 11 of the GDPR provides for sanctions in the event of non-compliance, thus ensuring consistent and rigorous data protection across the Union.

Thus, to be lawful, the processing of personal data should be based on the consent of the data subject or on any other legitimate basis provided for in the GDPR, including the need to comply with the legal obligation to which the data controller is subject.

4.2 Obligations of the controller

Taking into account the nature, scope, context and purposes of the processing, as well as the risks, of varying probability and severity, to the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and be able to demonstrate that the processing is carried out in accordance with the GDPR.

The controller must implement appropriate technical and organizational measures to ensure that, by default, only the personal data necessary for each specific purpose of processing is used.

This includes managing the amount of data collected, the scope of its processing, the duration of its retention and its accessibility (Article 25 RGPD).

In other words, the controller must ensure that personal data are not accessible to a wide audience without the explicit consent of the data subject.

These measures aim to limit the disclosure of data to what is strictly necessary, thus ensuring more secure management that respects the privacy of individuals.

Industry 4.0 technologies offer great flexibility and improved efficiency in industrial processes. However, they also expose companies to growing risks of cybercrime, particularly computer attacks. These risks include intrusions into critical systems, such as industrial control systems or central databases, which can have serious consequences, ranging from disruption of production to exposure of sensitive information.

In this context, a failure to protect personal data, such as a leak or misuse of collected information, can lead to liability for the data controller. As a result, organizations must implement technical and organizational measures to ensure data confidentiality and security (Féral-Schuhl, 2019).

Security obligations are multiplying and are becoming essential to prevent data breaches and ensure compliance with international standards.

4.3 Obligations relating to the security of processing

The GDPR imposes strict obligations on companies that process personal data, whether they are located in the European Union or process the data of European citizens. One of the key obligations is to implement appropriate security measures to protect personal data against data breaches, cyber-attacks or accidental loss.

Article 32 of the GDPR states that the data controller must "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk".

This includes, among other things, means to ensure the confidentiality, integrity, availability and resilience of the processing systems and services at all times; means to restore the availability of and access to personal data within a reasonable time in the event of a physical or technical incident; and a process to regularly test, analyze and evaluate the effectiveness of the technical and organizational measures to ensure the security of the processing.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of an individual, the controller shall notify the personal data breach to the data subject as soon as possible. Article 34 of the GDPR provides that notification to the data subject is not required if the controller has implemented appropriate technical and organizational security measures and these measures have been applied to the personal data affected by the breach, in particular measures that make the data unintelligible to anyone not authorized to have access to it, such as encryption. The controller must also take subsequent measures to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.

Paragraph 4 of the same Article provides that "if the controller has not already notified the data subject of the personal data breach concerning him or her, the supervisory authority may, after having assessed whether the personal data breach is likely to give rise to a high risk, require the controller to provide such notification". Finally, data controllers that are part of a Factory 4.0 affiliated to a central body may have a legitimate interest in transferring personal data within the group for internal administrative purposes (Wang et al., 2013), including the international transfer of personal data relating to customers or employees.

5. OBLIGATIONS RELATING TO THE INTERNATIONAL TRANSFER OF PERSONAL DATA BETWEEN 4.0 COMPANIES

Technologies have transformed both the economy and social relations and should further facilitate the free flow of personal data within the Union and their transfer to third countries and international organizations, while ensuring a high level of protection of personal data.

The flow of personal data to and from countries outside the Union is necessary for the development of international trade and cooperation.

However, in a framework where Factories 4.0 cooperate within a common industrial activity, they should be able to apply binding rules governing the transfer of personal data between their different entities, whether within the European Union or to other international subsidiaries.

These rules should ensure that all necessary precautions are taken to respect the fundamental principles of data protection (Guérin-François & Lessi, 2024).

In particular, they must include measures to protect the rights of individuals and to ensure an adequate level of security for the transfer of personal data, thereby ensuring compliance with the requirements of European data protection law.

5.1 Transfers based on an adequacy decision

This decision recognizes that the recipient country or entity ensures a level of protection for personal data that is equivalent to that in the European Union (An evaluation of criteria such as the respect for fundamental rights of individuals, local data protection laws, as well as available redress and security mechanisms).

When an adequacy decision is made, transfers can take place without the need for additional safeguards, such as standard contractual clauses (European Union, 2016).

However, this decision can be reviewed if the situation in the recipient country or organization changes, which could lead to a suspension of adequacy if data protection conditions change.

The adequacy of the level of protection takes into account, in particular, the rule of law, respect for human rights and fundamental freedoms, and relevant legislation, both general and sectoral (Balsmeier et al., 2017).

Second, the existence and effective operation of one or more independent supervisory authorities in the third country or to which a 4.0 factory is subject, responsible for ensuring compliance with data protection rules and enforcing them, including through appropriate powers of enforcement (Pagani & Pardo, 2017), assisting and advising data subjects in the exercise of their rights, and cooperating with the supervisory authorities of the Member States.

Finally, international commitments entered into by the third country or Factory 4.0 concerned, or other obligations arising from conventions or legally binding instruments, as well as from its participation in multilateral or regional systems, in particular with regard to the protection of personal data (Art. 45 RGPD).

In the absence of an adequacy decision, the data controller should, according to Recital 108 of the GDPR, take measures to compensate for the inadequacy of data protection in the third country by providing adequate safeguards for the benefit of the data subject.

5.2 International cooperation on data protection

With the rise of globalized technologies and cross-border data flows, it is becoming increasingly important to develop mechanisms that ensure the protection of individuals' rights beyond national borders.

In this regard, countries are working together to establish common standards and international agreements that facilitate data transfers while maintaining the confidentiality and security of personal information. Initiatives such as the EU's Adequacy Agreements are helping to create a harmonized framework for data management around the world.

In addition, these cooperation mechanisms include the establishment of specific safeguards and redress mechanisms to ensure that individuals can protect their personal data (Desgens-Pasanau, 2019) regardless of the country in which it is processed.

This cooperation is essential to meet the challenges posed by technological innovation while respecting the principles of privacy and data security in a globalized context.

The objective would be to develop international cooperation mechanisms to facilitate the effective enforcement of personal data protection legislation and to provide mutual assistance at the international level in the enforcement of personal data protection legislation, including notification, transmission of complaints, mutual assistance in investigations and exchange of information, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms, to involve interested stakeholders in discussions and activities aimed at developing international cooperation in the enforcement of personal data protection legislation, and finally to promote the exchange and documentation of personal data protection laws and practices, including with regard to conflicts of jurisdiction with third countries (Art. 50 RGPD).

6. CONCLUSION

In conclusion, Industry 4.0, as a force for digital transformation, requires a constant reassessment of personal data protection practices.
In the digital age, it is essential to implement appropriate compliance strategies to harmonize international standards and foster cooperation between EU and non-EU countries.

The challenges of securing personal data in Industry 4.0 with respect to the GDPR are numerous and complex, not least because of the interconnectedness of systems, the

vast amount of data collected, and the increased security risks. Companies need to implement robust data protection solutions, provide transparency to users, and ensure compliance with GDPR principles at all stages of the data lifecycle.

In this way, the synergy between the advanced technologies of Industry 4.0 and the protection of personal data is of paramount importance in order to protect the privacy of individuals while fostering innovation and economic growth within a secure framework that respects the fundamental rights and freedoms of individuals.

Acknowledgement: I wish to convey my profound appreciation to my esteemed friend, Mr. Amrani Ayoub, Doctor of Computer Science at Ibn Tofail University, for being the very first to ignite my passion for penning this article.

His unwavering support and belief in my endeavors were truly invaluable.

I would also like to express my heartfelt gratitude to my PhD supervisor, Dr. Mohammed Chakib Himmich, whose constant presence, wise guidance, and thoughtful feedback illuminated my path throughout this research. His expertise and encouragement were crucial in bringing this work to fruition.

A warm and heartfelt thank you extends to my beloved family, my parents, sisters, and brother for their steadfast support and boundless love. I am equally grateful to my fiancé for his patience, understanding, and emotional sustenance throughout this journey.

References:

Arroyo, J.-P., Brunet, S., & Sage, R. (2018). *GDPR and marketing: From constraint to opportunity*. e-thèque.

Balsmeier, B., Fleming, L., & Manso, G. (2017). Independent boards and innovation. *Journal of Financial Economics, 123*(3), 536–557. https://doi.org/10.1016/j.jfineco.2016.12.005

Bensoussan, A., Bensoussan, J., & Bonnell, B. (2016). *Comparative handbook: Robotic technologies law*. Larcier.

Blanchet, M. (2022a). *Industry 4.0* (1st ed.). Eyrolles.

Blanchet, M. (2022b). *The industry of the 21st century: The industrial champions of tomorrow: Agility, resilience, and responsibility* (1st ed.). Eyrolles.

CNIL. (n.d.). Phishing. https://www.cnil.fr/fr/cnil-direct/question/le-phishing-cest-quoi

Collin-Lachaud, I. (2022). *Revolutions of commerce in a transitioning society*. EMS Éditions Societing.

Desgens-Pasanau, G. (2019). *Personal data protection: The GDPR and the French law of June 20, 2018*. LexisNexis.

Donaldson, T., & Dunfee, T. W. (1999). *Ties that bind: A social contracts approach to business ethics*. Harvard Business School Press.

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data... (General Data Protection Regulation). *Official Journal of the European Union*.

Feillens, Y. (2024). *Industrie 4.0: Zero bullshit: The principles of 4.0 adapted to the real needs of your business*. Dunod.

Féral-Schuhl, C. (2019). *La protection des données personnelles* (1st ed.). Dalloz.

Guérin-François, A., & Lessi, J. (2024). *Code de la protection des données personnelles : annoté et commenté* (6e éd.). Dalloz.

Herschel, R., & Miori, V. M. (2017). Ethics & big data. *Technology in Society, 49*, 31–36. https://doi.org/10.1016/j.techsoc.2017.03.003

Hilary, G., & Serret, V. (2024). Governance and digital transformation. *Finance Contrôle Stratégie*. https://doi.org/10.4000/fcs.11653

Julien, N., & Martin, É. (2021). *The factory of the future: Strategies and deployment* (2nd ed.). Dunod.

Martin, K. E. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics, 137*(3), 551–569. https://doi.org/10.1007/s10551-015-2565-9

Ngombé, Y. (2024). *Digital law handbook* (2nd ed.). Ellipses.

Pagani, M., & Pardo, C. (2017). The impact of digital technology on relationships in a business network. *Industrial Marketing Management, 67*, 185–192. https://doi.org/10.1016/j.indmarman.2017.08.009

Plouin, G. (2022). *Cloud and digital transformation: Hybrid IS, data protection, anatomy of large platforms* (6th ed.). Dunod.

Reis, J., & Melão, N. (2023). Digital transformation: A meta-review and guidelines for future research. *Heliyon, 9*(1), Article e12834. https://doi.org/10.1016/j.heliyon.2023.e12834

Schaeffer, É. (2017). *Industry X.0: Creating value in the digital age* (1st ed.). Eyrolles.

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research, 24*(2), 201–218. https://doi.org/10.1287/isre.1120.0437

Drissi Imane
Ibn Tofail University,
Kenitra,
Morocco
imane.drissi2@uit.ac.ma
ORCID 0009-0000-4872-5463

Mohammed Chakib Himmich
Ibn Tofail University,
Kenitra,
Morocco
himmich.mohammedchakib@uit.ac.ma
ORCID 0009-0000-3208-880X