Anticipating compliance.  
An exploration of Foresight initiatives in data protection

By Alessandro Ortalda* , Stefano Leucci* and Dr. Gabriele Rizzo*

*Corresponding author, Ph.D. Candidate, Department of Interdisciplinary Study of Law, Faculty of Law and Criminology, Vrije Universiteit Brussel / Managing Director at Brussels Privacy Hub alessandro.ortalda@vub.be

* Stefano Leucci, Foresight Lead, Legal and Technology Officer at European Data Protection Supervisor / Fellow at Nexa Center for Internet and Society, Politecnico di Torino

* Dr. Gabriele Rizzo, Foresight executive, Independent / Member of the Board, Stakeholder Council of the Graduate School of Physics, Univeristà di Roma Tor Vergata
Acknowledgements

The authors thank Mr. Régis Chatellier and Dr. David Barnard-Wills for their precious contributions and reviews of this work.

Declaration of competing interests

The authors declare their professional involvement in the initiative Privacy For Futures, mentioned in section 4.4.

Disclaimer on the use of artificial intelligence tools

Generative artificial intelligence tools were employed in preparing this document. These tools were strictly used to revise existing content to improve clarity and ensure accessibility to a wider audience. The original content, research findings, and conclusions presented herein were developed independently and without direct generation from AI technologies.

The Brussels Privacy Hub publications are intended to circulate research in progress for comment and discussion. Available at https://brusselsprivacyhub.com/. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged.

DISCLAIMER

The opinions expressed in this paper are those of the author/s.
Abstract

The pace of technological progress has been increasing in recent years. As novel technologies arise or existing ones further develop, it becomes increasingly challenging to balance leveraging these advancements and safeguarding personal data. By relying on firsthand accounts of professionals in the field, the paper identifies how these challenges, which appear to be applicable to data controllers and Data Protection Authorities, are substantially connected with ensuring a sound interpretation of the law through time.

The paper examines the leading foresight and anticipation techniques and explore their possible data protection applications by reviewing existing initiatives that attempt to implement foresight in the context of data protection.

Section 2 delves into the evolving regulatory landscape, emphasising the need for a foresight-based approach to tackle the complexities arising from data-intensive technologies and the changing European regulatory framework. Section 3 introduces foresight as a discipline, its history and evolution, and leading techniques. Section 4 presents practical examples of foresight in data protection, detailing initiatives by the authors and other actors in the data protection space.

In conclusion, the paper underscores the initial consensus on the benefits of anticipatory approaches in addressing current data protection challenges. Anticipation techniques, as a flexible concept, can be tailored to meet the needs of various stakeholders, fostering a collaborative and practical approach to data protection. However, a gap in consolidated methodologies persists, necessitating further research to design and implement practical foresight approaches.

Keywords

Foresight; Anticipation; Data protection; GDPR; Data Protection Authorities; TechSonar; EDPS; CNIL; LINC; scenario analysis.
1 Introduction

The pace of technological progress has been accelerating in recent years. As novel technologies arise or existing ones further develop, it becomes increasingly challenging to balance these advancements with safeguarding personal data. The increasing number of digital platforms, interconnected devices, and the widespread use of data-driven services have created complex challenges for policymakers, businesses, and individuals. As society continues to rely heavily on technology, it becomes crucial to find practical ways to balance personal data protection with the fast pace of technological progress. In this context, developing and applying adequate capacities to anticipate and adapt to forthcoming developments can be instrumental in finding such balance. To this end, foresight and anticipation techniques\(^1\) have emerged to assist relevant stakeholders in making informed decisions and taking proactive actions. These techniques encompass various methods that help identify, understand, and assess possible future scenarios and their implications.

The goal of this exploratory paper is to examine the leading foresight and anticipation techniques and explore their possible data protection applications by reviewing existing initiatives that attempt to implement foresight in the context of data protection. By doing so, the paper hopes to bring scholarly attention to the topic and to kickstart a debate on how to achieve anticipation in data protection.

In section 2, the paper presents an overview of the current regulatory landscape, highlighting the main challenges that characterise it and suggests seeking solutions by moving toward a new foresight-based paradigm for data protection practices. In section 3, the paper introduces the readers to the history and main characteristics of the discipline of foresight and presents the leading and most common techniques used in this discipline. In section 4, the article surveys several current attempts to implement foresight into data protection, presenting in detail some of the initiatives carried out by the authors in preparation for this research.

---
The evolving regulatory landscape and its challenges

The proliferation of data-intensive technologies like artificial intelligence (AI) is driving increased data generation and availability\(^2\). Together with its many promises of benefits and societal advancements, these technologies can potentially introduce risks to the fundamental rights of individuals as well. This is particularly concerning if one considers, as scholars have emphasised, that individuals in a data-centric society can be characterised as inherently vulnerable\(^3\). In light of the growing availability of personal data, the improper use of this data can result in severe consequences for the rights of individuals.

Although the scale of the challenge is increasing exponentially, regulators have been working for the last 40 years to establish norms and safeguards that aim to balance the use of data with the protection of individuals’ fundamental rights. The effort can be traced back at least to the publication of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data\(^4\). In the European Union, the regulator continues down the path set by the Council of Europe, having passed laws on data protection such as the General Data Protection Regulation (GDPR)\(^5\), the Law Enforcement Directive\(^6\), and Regulation 2018/1725\(^7\).

However, today the European regulator is confronted by two pressing issues. The first one is the pervasive and ubiquitous use of data and the cross-domain nature of digital technologies. The need to address various scenarios and technologies led the European Union to intensify its endeavour to establish new laws and regulations. This is evident from the number of dossiers the EU is currently

---


\(^7\) European Parliament and Council of the European Union, ‘Regulation 2018/1725 on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data’, 23 October 2018.
working on⁸. The second issue the European regulator is confronted with is that the traditional “fact-based” approach to lawmaking seems incompatible with the fast-paced evolution of technology⁹. This might lead to a shortened lifespan for laws and their quickened transition into normative obsolescence. To address the challenge, the European regulator moved away from a prescriptive normative approach in favour of a more flexible principle and risk-based one¹⁰. This can be identified in several recent laws, such as the GDPR, the Digital Operational Resilience Act¹¹, the Network and Information Security Directive¹², and the draft of the Artificial Intelligence Act¹³.

The approach adopted by the European regulator – that is, increasing the number of laws and moving to a principle and risk-based approach –, while intended to address these issues, makes it more difficult to navigate requirements, increasing the complexity of reaching compliance for data controllers, and the complexity to enforce for data protection authorities (DPAs). First, many upcoming laws that regulate technology introduce new data protection requirements to be addressed. This requires constant monitoring of the evolution of the legal framework and a wide knowledge of requirements from a growing body of law. Certain actors, such as micro and small enterprises, might not be equipped to deal appropriately with this need in terms of available skills, resources, etc. Moreover, the possible risk of conflicting requirements within the EU normative framework¹⁴ and vis-a-vis extra-EU laws further exacerbates the issue¹⁵. Second, the risk-based approach – adopted, inter alia, to make the legal frameworks more adaptive and futureproof – creates ambiguity for data controllers¹⁶. Traditionally, compliance has been a relatively easy task,
especially in the context of a strictly prescriptive approach, where it can sometimes be reduced to a checklist exercise. However, in a risk-based framework, applying legal requirements can be less straightforward when compared to prescriptive legal frameworks\(^\text{17}\). In this setting, organisations must identify and understand the context in which they operate and implement measures coherent with it. For instance, according to Article 5(1)(c) of the GDPR, personal data should be processed in a manner that is "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed". Understanding what “adequate” and “relevant” mean is a contextual task left to data controllers. The same applies to the concepts of necessity and proportionality, which legislators intentionally left open-ended to allow for a constantly updatable legal text\(^\text{18}\).

This uncertainty should be worrisome for data controllers in two regards. First, concerning the alignment of their interpretation with the interpretation of DPAs. How can data controllers be sure that their interpretation of a legal requirement in a specific context can be considered “correct”? How can they be sure that enforcement agencies will understand the context in the same way, thus leading to the same interpretation of how to satisfy the legal requirement?\(^\text{19}\) This is a crucial aspect since DPAs have the power to impose sanctions for non-compliance situations that may arise from incorrect interpretations. Second, concerning the uncertainty of interpretation through time. How can data controllers be sure that the interpretation they give to a legal requirement in a specific context – and the compliance measures they implement to satisfy such requirement – will remain relevant in the future? How can they be sure that the context will not change in a way that makes the current interpretation of a legal requirement erroneous? The recent case of pseudonymised data is a helpful example of the relevance of such questions.

\(^{17}\) This issue is further exacerbated by the fact that the European legal framework interprets and adopts the risk-based approach in different ways, leading to what some scholars identified as regulatory fragmentation. See Giovanni De Gregorio and Pietro Dunn, ‘The European-Risk Based Approaches: Connecting Constitutional Dots in the Digital Age’, Common Market Law Review 59 (n.d.): 473–500.


\(^{19}\) An additional issue not explored in the present paper that might have consequences is the evolving perception of risks. Scholars have observed how data protection risks should be assessed considering the perception of data subjects. However, the perception of data subjects in regard to data protection risks might evolve over time, leading to uncertain assessment of risks. See for instance Timo Jakobi et al., ‘A Taxonomy of User-Perceived Privacy Risks to Foster Accountability of Data-Based Services’, Journal of Responsible Technology 10 (1 July 2022): 3, https://doi.org/10.1016/j.jrt.2022.100029.
Anticipating compliance. An exploration of Foresight initiatives in data protection

Since 2014, following the guidance of the Working Party Article 29\textsuperscript{20} (WP29), practitioners have widely considered pseudonymised data as personal data because it still retains the potential to be linked back to an individual\textsuperscript{21}. However, a recent landmark ruling by the European Court of Justice challenged this point by stating that if a recipient of pseudonymised data lacks the means to re-identify the data subjects, the pseudonymised data should not be considered personal data\textsuperscript{22}. This decision might have far-reaching consequences, impacting data storage, sharing, and processing practices across various industries. Businesses might need to reconsider their data handling strategies to align with this updated interpretation and ensure compliance with the evolving legal framework. Moreover, a set of guidelines addressing anonymity and pseudonymity\textsuperscript{23} is expected to be published in 2024 by the European Data Protection Board. This document, which will update the current interpretation stances from the WP29, might bring clarity or add uncertainty by moving the interpretation of the norms in yet another direction.

Another relevant example can be drawn by looking at data transfer agreements between the EU and the United States of America. In 2016, the European Court of Justice invalidated the Safe Harbour agreement due to its inadequate safeguarding of EU citizens' personal data in regard to personal data transfers to the United States\textsuperscript{24}. This insufficiency stemmed from the potential supremacy of U.S. surveillance laws over the agreement. Given the reasons for the initial annulment, it would have been relatively easy to predict the 2020 ruling of the European Court of Justice against the Privacy Shield, the instrument that took the place of the Safe Harbour agreement. Indeed, no significant alterations were made to the legal system in the United States, thus making the situation essentially unchanged from 2016\textsuperscript{25}. However, during the timeframe that separates the two rulings, organisations continued to operate following mostly ignoring the fact that a further annulment would be possible. The recently approved Data Privacy Framework, which came into force in 2023,

Anticipating compliance. An exploration of Foresight initiatives in data protection

still contains numerous crucial elements that are on par with the two previous annulments. Consequently, one might ask if this will face challenges similar to those of its predecessors. From the perspective of a data controller, this is an important question that can influence investments. From the perspective of DPAs, this is an important question that can influence enforcement activities in the future.

The examples of anonymisation and data transfer highlight that interpretation can change dramatically within brief timeframes\(^2\). This underscores the importance of comprehending and, to a certain extent, anticipating the evolution of legal interpretation.

Considering the increasing pace of technological and normative evolution, data controllers might get stuck in a never-ending race to identify and understand changes that occur in their context as these unfold and to update their interpretation of data protection requirements accordingly. Chasing these updates would be a monumental task, requiring a lot of resources and effort. This exposes data controllers to the risk of non-compliance from failing to adequately keep up-to-speed with changes and waste of resources that might ultimately undermine the effectiveness of the legal framework to safeguard the data protection rights of individuals.

The current situation is also a challenge for DPAs. The fast-paced technological landscape makes it difficult for them to provide timely and practical guidance to data controllers. As said above, DPAs’ interpretation is crucial for data controllers since it is the yardstick against which they can assess compliance. On top of this, DPAs are seen as among the most expert bodies on data protection, not only from a legal standpoint. They are often considered “the primary ‘disambiguators’ of data protection norms”\(^2\), making it even more relevant for them to be able to dispense data protection guidance and awareness. Moreover, DPAs seem to suffer from the reactive approach that is typical of enforcement bodies\(^2\). However, we contend this is misaligned with the risk minimisation

---
28 Scholars have investigated the distinction between reactive and proactive approaches by enforcement agencies, such as in the context of financial reporting, identifying the reactive approach as the most commonly employed. See Jochen Zimmermann, Jörg R. Werner, and Philipp B. Volmer, ‘The Stronghold of the Nation State: Enforcement Agencies’, in *Global Governance in Accounting: Rebalancing Public Power and Private Commitment*, ed. Jochen Zimmermann, Jörg R. Werner, and Philipp B. Volmer (London: Palgrave Macmillan UK, 2008), 120–42, https://doi.org/10.1057/9780230582866_7.
endorsed by the risk-based data protection framework and the “effectiveness” requirement that is part of the “data protection by design” principle in Article 25, GDPR\textsuperscript{29}.

We argue that the traditional reactive approaches to data protection needs to change towards proactive and anticipatory ones. This would involve developing a forward-thinking mindset that could help to anticipate changes and inform on plausible interpretation scenarios that might unfold in the future, leading to more effective data protection and safeguarding of fundamental rights. We believe this capacity, which seems absent from the skillsets and toolsets of the vast majority of data controllers and DPAs, can be pursued through foresight and future studies.

3 Foresight and anticipation

3.1 History and evolution of foresight

The discipline of foresight emerged in the aftermath of the Second World War as a decision-making tool in the military space. The race to nuclear armament that started after the conflict made military leaders realise that a reactive approach was not feasible anymore. The anticipation of – rather than reaction to – threats became the strategic objective to pursue.

Foresight emerged through the work of three paramount figures: General Henry "Hap" Arnold, the founding father of the U.S. Air Force; Theodore von Kármán, the forerunner of supersonic, hypersonic, and space flight; and Vannevar Bush, the initiator of the Manhattan Project. Their contribution led to the creation of the RAND project (later the RAND Corporation), a research and development effort created in 1946 to support the United States Air Force to, among other things, examine and study “the relative value of alternative strategies, tactics, instrumentalities, and techniques for future air warfare for the purpose of providing analytical information to assist the Air Force in formulating development plans and improved operational and logistical concepts”\textsuperscript{30}.

Experts at RAND understood that the future exists in the plural – as futures – and that futures are imagined not to be known – knowing the future would mean to “predict” rather than to anticipate, and foresight experts reject the possibility to predict the future – but to be used as tools for decision-making. Modern foresight is built on these fundamental premises.

In the last quarter of the 20th century, foresight became increasingly multidisciplinary, incorporating elements from disciplines like sociology, psychology, economics, and environmental sciences. After a few years, foresight techniques started to find an application beyond the military sector, such as in manufacturing, finance, healthcare, education, and others. A prominent example of this is the case of the Shell Corporation during the 1970s oil crises when a combination of geopolitical factors caused a shortage in oil supplies and a spike in prices that reverberated through many geographies and sectors of the economy. The British oil and gas company minimised the effects of these shocks by employing several foresight techniques that did not lead to predicting the crises but were instrumental in building up the resilience that ensured Shell weather the storm.

Technological advancements occurred in the last decades, particularly the emergence of Big Data and generative AI, have called for another evolution of foresight. Thanks to the availability of vast amounts of data, foresight practitioners have the opportunity to get comprehensive views of current and emerging trends, and thus access deeper and more efficient environmental scannings and trend assessments. Integrating artificial intelligence approaches has allowed for the automated analysis of vast data sets and the identification of intricate patterns, all helpful to understand weak signals and hidden variables in wicked problems, enriching foresight professionals’ capacity to explore the tradespace of futures under investigation while at the same time describing more organic images of the future.

Generative artificial intelligence and large language models have as well brought about new and fascinating opportunities in foresight. When aiming to create sets of scenarios to get to “roughly good” insights for decision-making, with speed of the process being paramount with respect to quality of results, the usage of such technologies offer interesting alternatives to create ready-made

---

sets of “instant scenarios”. Instant scenarios can also be used as an augment to framing, futuring, and visioning steps in the foresight competency model, enhancing foresight capabilities.

3.2 How foresight is implemented

Foresight is the capability to illuminate the broadest volume of possibilities, trends, and themes to be in the futures, to anticipate long-term decisions and prevent the loss of strategic advantage. As such, foresight helps organisations to anticipate the future by providing a structured approach to decision-making. Among the vast array of tools and techniques available in foresight to use the future, a category is that of scenarios, and related scenario planning. Scenario planning techniques help creating multiple scenarios for the future, so that organisations can, for instance, test the robustness of their strategies and identify potential weaknesses.

Scenario planning was introduced by Peter Schwartz, and is structured around building scenarios shaped by different forces of change and uncertainties. Scenario planning then evolved to more structured approaches, with a common one being the so-called “two-by-two”, or “2x2” for short. This scenario planning technique is used to build systematically four different future scenarios using two critical uncertainties as main directions for this decomposition. It requires diverse perspectives in scenario-building, encourages collaboration among experts, stakeholders, and other parties. This diversity is crucial to capture the wide range of forces that can shape the future.

Horizon scanning is another technique commonly employed to understand potential future forces of change by foresight professionals. It involves systematically monitoring and analysing the environment for signals of change, the so-called “pockets of future in the present”. As sci-fi author William Gibson said, “the future is already here: it’s just not evenly distributed”. By identifying potential disruptors early, organisations can take proactive steps to adapt and respond to changing conditions.

---


4 Foresight in data protection

To assess the potential applicability of the foresight discipline in developing an anticipatory approach to data protection, the authors undertook three distinct endeavours. These include the TechSonar project by the European Data Protection Supervisor (EDPS), a roundtable discussion on anticipatory compliance organised by the Vrije Universiteit Brussels (VUB), and a workshop on anticipatory enforcement jointly conducted by the EDPS and Brussels Privacy Hub (BPH). These initiatives involved stakeholders from many sectors, including the private sector, academia, non-governmental organisations (NGOs), and DPAs. They were deliberately designed to be distinct from each other, allowing for the testing of a wide range of implementation approaches. The present section describes these initiatives and others undertaken by various stakeholders, aiming to offer an initial assessment of the current state of foresight in the field of data protection.

4.1 TechSonar

The TechSonar initiative is a horizon-scanning exercise from the EDPS. It is built on a five-step framework established by the EDPS to identify and monitor a specific cohort of developing technologies that can potentially influence the safeguarding of personal data in forthcoming times.

EDPS has been exploring the benefits and possible uses of foresight for years. In its 2020-2024 strategy, the EDPS recognised foresight as its primary strategic pillar. This commitment to foresight can be understood by considering the responsibilities of the EDPS formalised in Regulation (EU) 1725/2018. Accordingly, one of the tasks of the EDPS is to “monitor relevant developments, insofar as they have an impact on the protection of personal data, especially the development of information and communication technologies”.

As of the publishing date of this paper, the EDPS has published three TechSonar reports. Currently, no scientific studies examine the outcomes and impact of TechSonar. However, the EDPS reports...
that it “contributed to put foresight in the spotlight and caught the attention of the data protection community”\(^4^3\). While more research is needed, this statement from the EDPS seems to be confirmed by informal discussions the authors held with representatives of the data protection field across different sectors. Accordingly, foresight remains a niche topic, but the work from the EDPS has brought the discipline to the attention of data protection specialists.

4.2 Roundtable on anticipatory compliance

On the 31\(^{st}\) of March 2022, the authors organised a roundtable discussion that brought together participants from the private sector, academia, NGOs, and DPAs. The primary aim of the roundtable was to ascertain and elucidate with concerned stakeholders the issues and challenges that characterise the current data protection landscape and examine the significance of anticipation and foresight in addressing these issues or reducing their potential hazards\(^4^4\).

During the discussion, the participants expressed concerns about the lack of predictability in the current situation. The consensus among the group was that the practical application of general data protection principles poses a significant challenge. Due to the contextual nature of the principle and risk-based framework, numerous participants experienced a sense of being overwhelmed by the diverse range of criteria involved. Criteria such as the different socio-cultural models across different geographies and communities were presented among the obstacles to compliance. In particular, the rapid pace of change in the current scenario was seen as a matter of concern. Participants pointed out how the evolution of technology is accelerating together with the regulatory framework, with new sets of requirements emerging in short timeframes. Representatives of DPAs, in particular, raised concerns regarding the potential decline in their ability to offer timely and practical guidance in response to the ongoing challenges posed by rapid technological advancements.

Following a comprehensive discussion, the authors suggested using foresight to tackle the abovementioned challenges. Most participants had not been previously exposed to the discipline of foresight, and a nearly unanimous agreement arose regarding the advantages such an approach can

\(^{43}\) European Data Protection Supervisor, *TechSonar*, 3.
\(^{44}\) The activity was conducted within the European project PANELFIT, funded under the Horizon 2020 program. Participants comprised 3 academics with extensive knowledge in the field, 2 professionals from privacy authorities who provided crucial regulatory perspectives, 2 representatives from non-governmental organizations (NGOs) committed to safeguarding individual rights, and finally, 4 experts from the private sector who brought valuable skills and a practical approach. This diversity of perspectives and expertise enabled a combination of diverse viewpoints. More information can be found here: [https://www.panelfit.eu/](https://www.panelfit.eu/)
Anticipating compliance. An exploration of Foresight initiatives in data protection

offer to data protection and compliance. The group praised the prospect of establishing a methodology for anticipating changes rather than reacting to them. Furthermore, the participants appreciated the cooperative and practical nature that various foresight methodologies entail. They expressed a belief that this approach could foster enhanced collaboration among data controllers, DPAs, civil society, and regulators. Additionally, they argued that it could facilitate the development of a more harmonious, inclusive, and transparent data protection ecosystem among stakeholders who frequently view each other as adversaries.

During the workshop, the group coined the term “Anticipatory compliance”. Although the group could not reach a consensus on its formal definition, all participants made themselves available to be involved in future works to design this approach in practice.

4.3 Anticipatory enforcement workshop at the EDPS Conference

In June 2022, the authors organised a workshop to explore potential applications of anticipatory compliance in data protection enforcement. This occurred during the annual conference hosted by the EDPS45, which sponsored the workshop as part of its strategy to implement foresight initiatives. The authors were motivated to explore the ideas that emerged during the roundtable on anticipatory compliance held in March, focusing this time on the enforcement aspects of data protection and how these can influence the behaviour and actions of concerned stakeholders. To do so, the authors designed the workshop as a practical exercise to simulate speculative scenarios depicting the implementation of different approaches to data protection enforcement in Europe and to collect feedback and insights from participants about their consequences.

The workshop saw the participation of 18 individuals, including some attendees who had previously participated in the March roundtable on anticipatory compliance. To ensure diverse perspectives, participants were selected from various sectors, including academia, the private sector, the public sector, DPAs, and civil society. The workshop was designed as a practical tabletop scenario simulation informed by a revised version of the 2x2 method46. The authors created the four fictional scenarios set in the year 2030 and designed around the interplay of two forces of change: the

46 See section 3.2.
“proactiveness” of DPAs in their enforcement actions and the “distribution” of enforcement power across the European governance system.

In the scenarios, “proactiveness” means the ability of DPAs to anticipate emerging phenomena and use this understanding to plan and execute their enforcement activities, while “distribution” pertains to the governance structure of DPAs from highly centralised models featuring a singular authority at the European level to a completely decentralised approach, with individual authorities in each member state. The convergence of these two forces of change yielded four distinct scenarios, each portraying a diverse outlook for 2030. The discussion focused on the potential hazards and challenges associated with each scenario and explored possible ways to address them.

At the end of the exercise, the authors presented the concepts of anticipatory compliance. They engaged participants to express their views in light of the practical exercise they had just concluded. The outcomes of this discussion aligned with those from the previous roundtable in March, with participants welcoming this new anticipatory approach as a potential solution to current issues and deeming it worthy of further investigation.

The discussion predominantly centred on practical implementation aspects but also touched on the characterisation of what “anticipation” means in the context of data protection. According to the debate, anticipation can be described as the proactive capability to ensure early detection of risks from specific data processing activities while considering possible socio-technological evolutions of the scenarios. The description is crucial because it systematises and aligns several elements.
Anticipating compliance. An exploration of Foresight initiatives in data protection

discussed extensively in the March roundtable and the June workshop. Two are of particular relevance. First, this description acknowledges anticipation as a “capability”. As such, practitioners need to develop, train, and hone anticipation. This is one of the pivotal points in the foresight discipline, so important that it has spurred the creation of a whole branch of foresight called “future literacy”, which focuses on how to cultivate a forward-looking approach. Second, the definition clearly identifies anticipation as an instrument to understand and manage risks. As such, it can be effectively considered a measure that data controllers can put in place to minimise the risk of data processing.

Although the output of the workshop did not produce a concrete and implementable foresight approach to data protection, it provided the authors with concrete elements to continue their research on how to design and implement such practical approaches to anticipatory compliance.

4.4 Other initiatives

Although the adoption of foresight and anticipation in data protection is still relatively niche, there are initiatives carried out by private and public entities. For instance, the French DPA (Commission Nationale de l’Informatique et des Libertés – CNIL) established the Laboratoire d’Innovation Numérique de la CNIL (LINC). The LINC focuses on emerging digital technologies and data usage trends to stimulate debates on ethics, freedoms, data, and digital use. The LINC adopts a hands-on approach that involves collaboration with expert groups to analyse potential developments and propose innovative and creative solutions to tackle new challenges. Since 2011, even before its formal creation in 2016, LINC has been actively involved on several topics, such as the evolution of financial services and systems, the concept of the "Smart City," the so-called “civic tech”, and cookies enforcement.

---

Anticipating compliance. An exploration of Foresight initiatives in data protection

In the United Kingdom, the Information Commissioner’s Office (ICO) recently initiated the “Tech Horizons Report” series\(^{50}\). These analyses try to assess and anticipate the evolution of certain technologies over the short, medium, and long term.

The private sector also presents cases of foresight applied to data protection. For instance, the global consulting firm Deloitte has launched a service called “Regulatory Sensing”\(^{51}\), which aims at detecting and monitoring regulatory changes and anticipating compliance requirements. This service leverages technology to collect and analyse data, providing real-time tracking, early warning, and mapping services for changes in the regulatory landscape. Another example is the new “Privacy For Futures” initiative\(^{52}\), which, to the author’s knowledge, is the first and only initiative attempting to introduce concrete and methodologically sound foresight techniques in data protection.

5 Limitations and future research

This paper has examined the incorporation of foresight and anticipation methods in data protection, with the goal of promoting a mindset of "anticipatory compliance" among different stakeholders, such as data controllers and DPAs. The results emphasise the potential advantages of employing foresight in effectively navigating the digital and regulatory environments. However, it is important to acknowledge that there are certain limitations and areas that warrant further investigation.

First, the focus on the European regulatory framework, although relevant given its extensive scope and worldwide impact, may restrict the generalizability of findings to other jurisdictions characterised by distinct legal and cultural perspectives on data protection. New studies should attempt to broaden the research scope to encompass comparative studies on the implementation of foresight and anticipatory approaches to data protection in jurisdictions beyond the EU.

Second, this study predominantly relies on firsthand testimonies collected during workshops and initiatives that directly employ foresight in data protection. Both these categories provided a limited amount of evidence to be assessed. This might be due to the infancy of this field of foresight in data protection, a conclusion that the overwhelming lack of academic work on the subjects might further


Anticipating compliance. An exploration of Foresight initiatives in data protection

strengthen. Although the blend of firsthand testimonies and analysis of existing initiatives offers valuable insights, it is deficient in terms of a comprehensive empirical foundation that could provide a more thorough understanding of the role of foresight techniques in developing anticipatory compliance. This is of particular relevance, considering that the discipline of foresight encompasses a diverse array of methodologies, each possessing distinct advantages and disadvantages. This paper lacks an in-depth examination of the most appropriate foresight methodologies for data protection, as well as an exploration of how these methodologies can be customised to tackle the distinct challenges of the field.

Future research has the potential to make a substantial contribution to the comprehension of the significance of foresight in data protection and the improvement of the practical implementation of anticipatory compliance strategies. Subsequent investigations should focus on identifying, creating, and empirically evaluating particular foresight methodologies that are most appropriate for addressing the distinct difficulties associated with data protection. This entails assessing how these methodologies can be customised to suit the requirements of various stakeholders.

6 Conclusion

Given the complexities and challenges outlined in the preceding sections, the limits of a purely reactive approach to data protection emerge clearly. The swift pace of technological advancements, coupled with the evolving regulatory framework, requires a forward-looking approach. One candidate to develop such a forward-looking approach seems to be found in the discipline of foresight and its use of anticipation as a tool. Indeed, drawing from the preliminary experiences described above, there seems to be a possible – yet relatively small, given the absolute number of professionals involved – consensus on the benefits of anticipatory approaches to tackle the current data protection challenges. While not definitive, this consensus suggests that more investigation in this area is necessary.

Anticipation also appears to be a flexible concept that can be adapted to the needs of different stakeholders. DPAs can use it to provide timely and valuable guidance to other parties, while data controllers can use it to make their compliance programmes more effective.

Anticipation techniques can also serve as leverage to align the needs of these actors, fostering a more collaborative and practical approach to data protection. By acknowledging and addressing
each actor’s unique problems, it is possible to work towards a more robust and adaptable system of data protection that is equipped to respond to the complex and ever-changing digital landscape.

However, the lack of a consolidated methodology makes it difficult for concerned stakeholders to develop such capabilities. Initiatives such as the TechSonar project attempt to draw value from foresight and provide insights into potential future challenges. However, these initiatives, while informative, stop short of offering a practical process for implementing anticipatory capabilities. Recognising this gap, it becomes essential to transition from theoretical discussions to developing actionable frameworks that organisations can adopt to integrate foresight into their data protection practices effectively.

We conclude by pointing out the need for further applied research, which should be conducted to design practical implementation approaches of foresight in data protection.

7 Bibliography


Anticipating compliance. An exploration of Foresight initiatives in data protection


———. ‘Regulation 2018/1725 on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data’, 23 October 2018.


Anticipating compliance. An exploration of Foresight initiatives in data protection


Anticipating compliance. An exploration of Foresight initiatives in data protection


