The legal sources of the EU's General Data Protection Regulation: Compliance, environmental regulations and liability for faulty products

Winston Maxwell
&
Christine Gateau,
Attorneys, Hogan Lovells

Abstract:
The EU's General Data Protection Regulation (GDPR) draws on the general principles of consumer protection adopted over the past forty years. However the scope of these principles has been expanded, in particular with regard to sanctions and the provisions on corporate liability. The GDPR has drawn from the US concept of compliance and from environmental regulations, in particular those about the operation of "sensitive" (high-risk) industrial plants. The obligations imposed on firms leave room for interpretation and flexibility: how to define an "appropriate", "fair" or "non-excessive" handling of data? These flexible concepts of liability under civil law receive an economic application via the "Hand rule". Firm are responsible for setting the right level of protection by taking account of the risks and costs of protective measures. The registry and impact assessment foreseen by the GDPR are decisive documents for proving that they have done so. As for liability, the GDPR draws on rules for defective products. The provisions foreseen by this regulation will expectedly converge with those adopted for risk management in firms.

The EU's General Data Protection Regulation (GDPR)[1] relies on the same principles as EU Directive 95/46, which are also found in the 1981 Convention 108 of the Council of Europe and in the 1980 OECD guidelines (as modified in 2013). These same principles figure in the 1978 French Act on Informatics and Liberty and the 1974 US Privacy Act.[2]

The basic principles have not fundamentally changed since forty years ago. In the wording of the GDPR, data have to be handled "*lawfully and fairly*", collected for "*specified, explicit and legitimate purposes*"; they have to be "*accurate*", and stored for a period no longer than necessary for the purposes for which they have been recorded.

Nevertheless, the GDPR marks a break with the past since it foresees arrangements for holding firms responsible and a system of dissuasive sanctions stricter than any previous measures concerning personal data. What has changed is the scope of risks — and opportunities — related to the uses of data. To be effective, the GDPR had to change scales. Data have become a major subject for compliance with the law — like legal rules against corruption, competition law, environmental regulations and regulations about dangerous installations. The GDPR signals an awareness similar to what happened following the *Amoco Cadiz* oil spill in 1978 and the Seveso disaster in 1976. In fact, it draws on the regulations for installations classified as "seveso", since its provisions on the traceability, storage and use of data are adjusted as a function of the level of

[1] The GDPR (General Data Protection Regulation): "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data". Available via: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478961410763&uri=CELEX:32016R0679.
[2] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.

potential "toxicity". The data user has to identify the risks from the very start and draw up measures of security for installations under the supervision of regulatory authorities. Data of a personal sort have become indispensable in the economy; but like oil or other chemicals, they can give set off major negative externalities that call for strong regulatory interventions.

In Europe, personal data are both a fundamental right and an object of commercial transactions. The GDPR tries to conciliate these two aspects. Its objective is to facilitate the free circulation of personal data and their use by firms. At the same time, the GDPR reminds us that these data are not a commodity (merchandise or service) like others. It tries to manage this tension, along with the tension between various fundamental rights. A measure that provides more protection to personal data might hamper the access to information or infringe on private property rights. In cases of friction between several sources of law or fundamental rights, a rule of proportionality applies for limiting each interference to what is absolutely necessary.

A direction: The principle of accountability

Under the GDPR, a firm has to set up its own arrangements for performing risk assessments and drawing conclusions about the processing of data and about whether the measures for doing so are fair, unexcessive and adequate. These in-house arrangements entail keeping a register of the processing of personal data. Besides listing each action of data processing in this register, the firm has to identify the data-processors and subcontractors as well as any international transfers of data. Above all, the register has to precisely describe the purpose for which the firm is processing data. This register is the keystone of the system for holding the firm accountable. It identifies the processing of sensitive data and, too, data-processing for which the purpose is vague or poorly defined or which rely on subcontractors or involve unauthorized international transfers.

The register imposes a rationale of traceability, as in the case of managing dangerous substances in a factory. For regulatory authorities, the absence of a register or lack of full information therein automatically amounts to a violation. The same holds if the register lists an act of data processing that carries risks and if data processor does nothing to reduce this risk.

An advantage of the register is that it forces firms to ask themselves the right questions. What are the legal grounds for an act of data-processing? What about the individual's consent or the firm's legitimate interests? Does the processing ensue from a contract? Is the purpose sufficiently clear and legitimate? Are the data collected germane to this purpose? Have "*the data subjects*" received full information about the processing? How does the firm see to it that individuals may exercise their rights of access to their data, of rectification, of deletion and of portability? What security measures has the firm taken? How have data transfers been organized within the firm, with partners and subcontractors?

Using the register and this list of questions, the firm will make an initial assessment of both the risks and the measures in compliance with the law for mitigating them. This assessment is the occasion for it to prove that it has complied with the conditions set for low- or mediate-risk data-processing. When the firm concludes that the processing entails high risks, it will have to make a detailed impact assessment. As under the EU's "Seveso 2 directive",[3] the GDPR induces firms and regulatory authorities to concentrate on high-risk cases. This impact assessment will be an important document for proving compliance with the law.

These requirements reverse the burden of proof. Henceforth, the firm has the responsibility of proving it has taken all appropriate measures for protecting the personal data in its possession and respecting people's rights.

[3] Texts of European Union law are available via http://eur-lex.europa.eu/browse/directories/legislation.html; & texts of French law, via: https://www.legifrance.gouv.fr/Droit-francais.

A guideline for "appropriate measures": The principle of proportionality

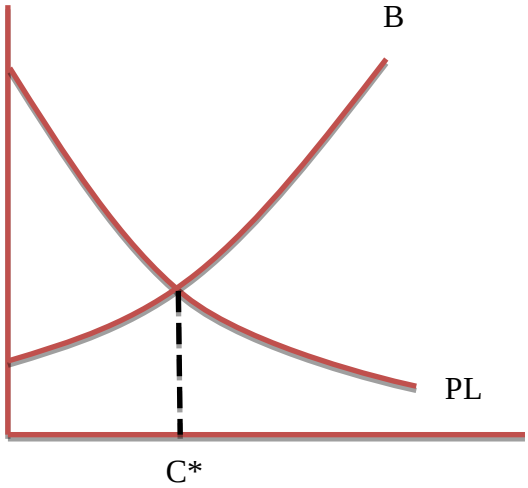
Applying the GDPR will be a balancing act — this balancing of competing (or even contradictory) rights and interests lies at the core of key concepts such as "*appropriate technical and organizational measures*", "*legitimate interests*" and "*fair processing*". These concepts allow room for firms, regulatory authorities and judges to maneuver so as to shift the cursor as a function of the context and of the risks to individuals. They will be interpreted differently in the cases of a small business, which manages a database with information on a few hundred customers, and of a giant of the Internet, which manages data on millions of consumers.

Given the many zones of friction, lawmakers have adopted a variable approach depending on the case and risk. Apart from a few typical cases, the GDPR offers no unequivocal, binary response. It lays down the principle of "appropriate measures", a flexible concept similar to the phrase "like a good father and head of household", which used to figure in the French Civil Code but has now been replaced with "reasonable". The GDPR emphasizes the means firms implement to responsibly manage personal data. This emphasis on the organizational and technical means of protection evokes the concept of compliance. For instance, US authorities require the implementation of compliance policies that are effective in the fight against corruption and in relation to competition law. The EU regulation draws directly on this tradition. Firms have to implement the appropriate means by taking account of: the risks to individuals, the state of technology, and the costs of implementation. The intent is for a reasonable instead of absolute protection.

But what constitutes reasonable protection? The impact assessment foreseen under Article 35 of the GDPR resembles the risk analyses performed by firms for the safety of products before placing them on the market. In an economic analysis, reasonable measures correspond to the point of maximization of social well-being. Drastic protective measures can impoverish society. For example, a speed limit set at 30 km/hr would reduce the number of casualties in accidents and, too, strongly reduce the utility of cars. In like manner, a regulation that holds platforms responsible for all contents posted by users would motivate the platforms to drastically limit on-line information; and this would limit the freedom of expression. Each regulation and protective measure has secondary effects that have to be taken into account to determine the optimal level of regulation.

In economic terms, the appropriate level of protective measures corresponds to the point where the marginal cost of an additional unit of protection is equal to the protective measure's marginal benefit. Beyond this point, additional safety measures cost society more than the benefits produced. They then reduce overall social well-being instead of increasing it. This formula, the so-called "Hand rule", stems from a decision in 1947 made by Judge Learned Hand in a US court. Since then, it has been used to calculate negligence. In Figure 1, the optimal level of protective measures is at C^*.

Figure 1: Graphic of the Hand rule: The marginal cost of additional protection

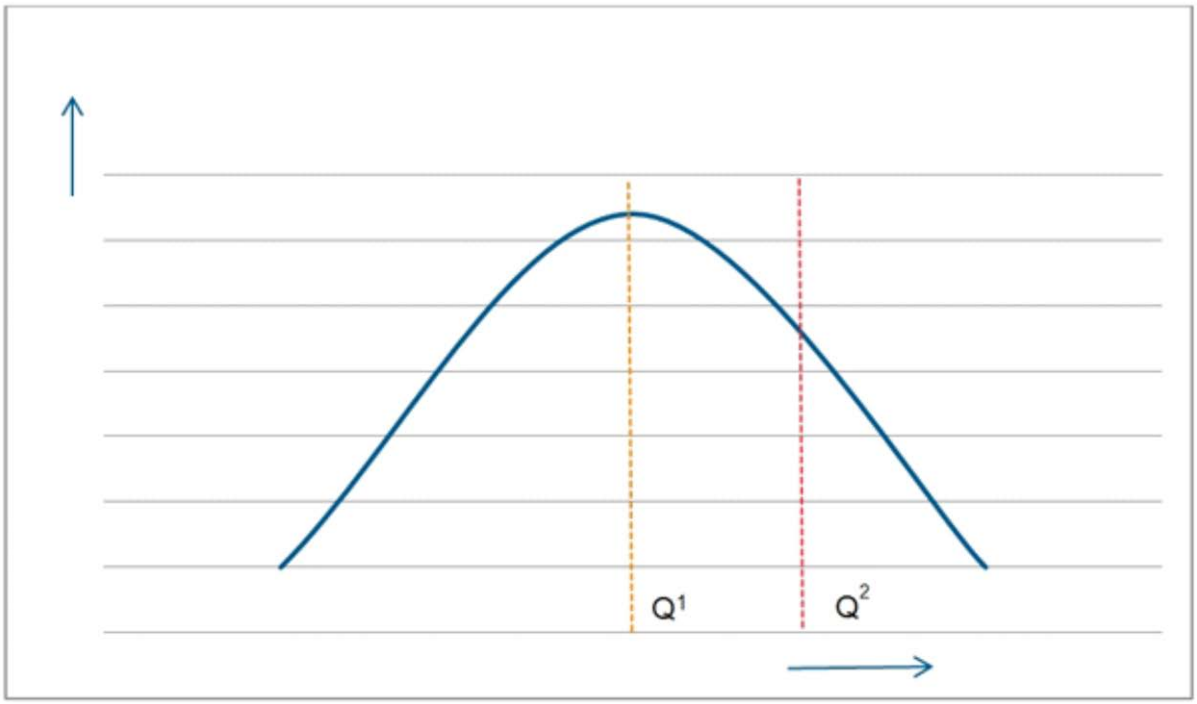


Costs (y-axis), number of protective measures (x-axis)
Marginal cost of protective measures (B)
Marginal cost of averted injury (PL)

Source: POSNER (2011)

In Figure 1, the curve *PL* represents the costs linked to the risk of injury, *P* is the probability of the occurrence of an injury; and *L*, the harm resulting from its occurrence. To take an example: if the social cost (*L*) of the loss of a million credit cards equals €100 million (€100/card) and the probability (*P*) of this loss is 0.1% (one out of a thousand), the product *PL* will be €100,000. The curve *PL* decreases as protective measures are adopted but it does not reach zero: it flattens out. This means that, beyond a certain point, each additional protective measure does not decrease the risk as much. The curve *B* represents the costs of protective measures. In general, the first such measures, which are not expensive but are very efficient, have a major impact on risk (decreasing *PL*). Beyond a certain point however, protective measures are costly and do much less to decrease risks. For example, a protective measure that reduces the probability (*P*) from 100% to 0.5% might cost as much as an additional measure that reduces the probability from 0.5% à 0.1%, or from 0.1% to 0.08%. The cost of each increment of protection increases as we approach zero risks. The curve *B* rises exponentially.

Figure 2: Maximizing social well-being (y-axis) as a function of the efficiency of protective measures (x-axis)
Source: MAXWELL (2017)



The graph in Figure 2 presents another depiction of the optimum of protection. It shows the point at which social well-being reaches a maximum. Even though the preventive measure Q_2 offers a higher level of protection than Q_1, the optimum is Q_1, where social well-being is maximal.

The impact assessment foreseen under Article 35 of the GDPR will shed light on both the risks and the measures to be implemented to reduce them. Corporate leaders will have to decide what is the acceptable level of residual risk, a decision dependent on the firm and on practices in the industry. If, for example, data are leaked, the firm will have to justify its decisions by proving (with the impact assessment) that the measures taken were reasonable even though they did not reduce risks to zero.

At the end of the road: Applying a strict concept of accountability to "controllers and processors"

The GDPR imposes a strict conception of responsibility on the parties in charge of data-processing: once a violation is established, redress will be automatic. The "*data subjects*" who are affected may bring an action without having to prove the fault or negligence of the party in charge of the processing. Under Article 82-3, "*a controller or processor shall be exempt from liability […] if it proves that it is not in any way responsible for the event giving rise to the damage*"; but the burden of proving that the processing of personal data complies with the GDPR (and its transpositions into the law of member states) clearly falls on the controller of the data.

Furthermore, firms have to be prepared: the "*data subjects*" who are affected may bring an action before regulatory authorities in order to obtain access to the conclusions of the administrative report — which they will likely use in a civil action suit. Given this approach, these persons can easily justify a presumption of a violation of their personal data. As a consequence, a heavier administrative burden falls onto the "*controller and processor*" of the data.

The GDPR's provisions for holding "*data controllers and processors*" accountable require that defendants prove they have taken "*appropriate technical and organizational measures*". Controllers and processors must translate these provisions into a pre-litigation strategy for creating the documents that will enable them to prove they have taken "*appropriate technical and organizational measures*". The register of data-processing operations and the impact assessment will be decisive for rebutting the presumption that weighs on them.

Conclusion

We can expect a convergence between, on the one hand, the procedures firms adopt to handle the risks related to the GDPR and, on the other hand, the risks related to product safety or pollution. Risk and impact assessments will become similar, thus fostering a pooling of expertise in the firm around risk management and the preparation of impact analyses. The firm's GDPR program will then be incorporated into its general arrangements for managing risks within its organization

References

MAXWELL W. (2017) *Smarter Internet Regulation through Cost-Benefit Analysis: Measuring Harms to Privacy, Freedom of Expression and the Internet Ecosystem* (Paris: Presses des Mines).

POSNER R.A. (2011) *Economic Analysis of Law*, 8th edition (New York: Aspen Publishers).