Bloor

InContext

InContext Paper by Bloor
Author **David Norfolk**
Publish date **June 2023**

Information privacy compliance – *personal data protection issues, for EU GDPR in particular*

Information privacy law usually now has real teeth: in the case if EU GDPR the maximum fines or non-compliance are €20,000,000 or 4% of the previous year's worldwide turnover, whichever is greater.

Introduction

There is a new story for business automation to deal with these days: information privacy. The most obvious example of this, since May 25th, 2018, is EU General Data Protection Regulation (GDPR) compliance, but it is actually a more general, and global, issue. GDPR regulates the security and use of the personally identifiable information (PII) of EU citizens, but it has been made a model for similar regulations worldwide.

These laws are generally intended to return to people – data subjects – control of their own PII, but they also have an impact on the free movement of data, since it obviously makes no sense to regulate the privacy of PII in one country and provide free access to this PII in another country. So, information privacy laws generally prohibit export of PII to other countries unless the destination has equivalent information privacy protection laws. This means that information privacy laws will be implemented around the world, in the interests of facilitating trade. It is worth noting that information privacy regulation is bi-lateral. It is not enough for the UK, say, to implement a law called GDPR (as it has), the EU has to agree that the UK GDPR is equivalent to EU GDPR in the protection given to PII before EU PII can be sent to the UK.

Information privacy law usually now has real teeth: in the case of the EU GDPR the maximum fines for non-compliance are €20,000,000 or 4% of the previous year's worldwide turnover, whichever is greater. This means that compliance with Information Privacy laws such as GDPR matters. We will go into the technical detail of what this means below but, above this, you will be expected to maintain an effective privacy culture, with appropriate policies and procedures.

This InContext is intended for the managers, both business and IT, in any firm subject to information privacy laws. It will also be useful for staff involved in implementing or operating information privacy policies, processes, and procedures.

“These laws are generally intended to return to people... control of their own PII, but they also have an impact on the free movement of data, since it obviously makes no sense to regulate the privacy of PII in one country and provide free access to this PII in another country.”

Information privacy

There are many companies that will offer you help with demonstrating compliance with information privacy laws such as GDPR. Such help can be invaluable but you should remember that you can outsource execution, but you can't outsource accountability – you should read the relevant laws, and ensure that you really are compliant and understand what this means. Fundamentally, compliance is fairly simple, although there are devils in the detail. The EU GDPR says, on its ***website***: *"the data privacy principles of the GDPR are fairly straightforward. The law asks you to make a good faith effort to give people the means to control how their data is used and who has access to it. To facilitate this, you must transparently and openly provide them with the information they need to understand how their data is collected and used. And you have to make it simple for your customers and users to exercise the various rights (of access, of erasure, etc.)"*. If you are not compliant, you may well find it difficult to do business with people, such as those in the EU, who do take information privacy seriously.

In order to become compliant, you will first need to put in place a "privacy culture", that will allow you to demonstrate that you truly put the rights of your data subjects with respect to their personally identifiable information (PII) at the core of your organisation. Compliance is not a simple prescriptive checklist that you can pay lip service to.

There is also the issue of existing data, since data subjects are entitled to know the source of PII that you process, the purpose for which you are storing it and the time for which it will be kept. You have to have the consent of the data subject for processing personal data, and your existing databases probably don't contain fields for Consent, Source, Purpose and Time Kept. And suppose that Consent is rescinded, can you remove PII from your processing and archives?

Taking EU GDPR as an example, organisations that collect, process or store PII as part of their core activities should appoint a Data Protection Officer, to oversee PII management and provision of timely access to PII. They must also notify the supervisory authority in their country (in the UK, which implements its own version of GDPR, this would be the ***Information Commissioner's Office*** (ICO)) of any data breach affecting PII, within (typically) 72 hours.

The purpose of Information Privacy Law generally is to return control of personal data to individuals (data subjects), and to facilitate international business by creating a standard for PII treatment across the world. The EU GDPR came into full effect on May 25th, 2018, and it is serving as a model for similar privacy laws around the world.

"In order to become compliant, you will first need to put in place a *"privacy culture"*, that will allow you to demonstrate that you truly put the rights of your data subjects with respect to their personally identifiable information (PII) at the core of your organisation."

An information privacy solution

The vendor

IRI is a privately-owned ISV founded in 1978. Its offices are in Florida and it relies on a partner network of resellers for international coverage (in 40 locations throughout the world). Its key platform product is Voracity, a data management package designed to perform and consolidate common work in Data Discovery, Data Integration, Data Migration, Data Governance and Analytics. This platform includes three static data masking (SDM) products, to locate and protect PII; and reporting tools, needed to prove compliance with the requirements of GDPR and similar information privacy laws.

What is its information privacy offering?

The IRI GDPR offering, which will also support other information privacy laws worldwide, provides tools to facilitate the protection of PII, the discovery of PII and the "de-identification" (with pseudononymisation, redaction, anonymisation etc.) of PII. This data-centric security capability is supplied through 3 stand-alone static data masking (SDM) products, called IRI FieldShield, DarkShield, and CellShield, which are all also included components of the Voracity data management and governance platform (which includes data integration, migration, cleansing, reporting, and analytics capabilities as well). The offering also includes "learning resources", which is good, because information privacy is about so much more than just technology.

What does it do?

IRI GDPR solutions cover a wide range of the use cases associated with information privacy regulations, including the rights to erasure, portability, and rectification. Ultimately, it is all about promoting Trust – as David Friedland (VP of Business Development at IRI) says, *"if your customers don't trust you to look after their PII, you won't be in business for long"*. There are also many risks associated with mismanagement of PII. You can be exploited by external "bad actors", stealing your data or holding it to ransom; or internal bad actors (both dishonest employees or disgruntled employees); or careless employees. If someone knows that your internal PII is mismanaged and that you don't, perhaps, have an effective privacy culture, a simple and safe way for them to disrupt your business is to send in a lot of, quite legitimate, data subject access requests (DSARs), as data subjects have the right to see what PII you hold on them. If you haven't thought about this possibility before, deciding what information you must hand over and what you don't need to, and (in many cases) finding it, can waste a lot of time and resources.

Thus, the first IRI capabilities you should be interested in are its data discovery (search) features. You can't manage issues you don't now you have or comply effectively with regulations you don't fully understand and Friedland says that only about half of the people approaching it have the staff and the expertise for the job. So, IRI has a nice business around "data masking as a service", which includes data classification, profiling and location reporting, too.

Ultimately, however, the basis of IRI's compliance offering is data obfuscation (replacing identifying PII such as names or email addresses with misleading or random strings), pseudonymisation, encryption and similar data masking functions which serve as a means of "data breach mitigation". Even if information is looked at or stolen, the perpetrators can't do much with it and the regulators will see you as still being more or less in control of it.

Note that the manner and the extent to which data gets masked means you are engaging in risk mitigation or management, not risk elimination. Reversing de-identification is often possible, by correlation of other unmasked related characteristics (known as quasi-identifiers) of an entry

"...the basis of IRI's compliance offering is data obfuscation (replacing identifying PII such as names or email addresses with misleading or random strings), pseudonymisation, encryption and similar data masking functions which serve as means of *"data breach mitigation"*."

(e.g. if you know that there us only one billionaire living in the village of Little Snoring, it will be possible to identify her bank account from the village name); and if criminals hold your data, they can use extremely powerful computers to break your encryption. In fact, if you lose your encryption keys, you may lose PII (which isn't allowed) as effectively as if someone sabotaged the hard drive it was on. So, if you are to manage privacy risk successfully, you will probably need training and, possibly, consultancy, to help you attain "good practice" around what elements are masked and with what technique, based on the balance between data security and utility in the masked environment.

IRI maintains a considerable body of how-to articles and videos around data masking of structured, semi-structured, and unstructured data sources held on-premise or in the cloud, in its ***self-learning page***.

Once you have an information privacy culture in place and have thought about suitable policies and procedures, you will want to be able to find PII reliably, partly because of the possibility of DSARs. This can be non-trivial, especially as you'll need to look through unstructured data, possibly even emails and the like. IRI tools can help with the classification of data, so you can find it more easily, and the anonymisation of PII in such a way that referential integrity between related records is maintained. For example, medical admission and discharge dates, and birthdates, are all PII and should be anonymised when the data is used for testing, say – but the anonymised birthdate for a given patient must be less than her anonymised admission date, which must be less than her anonymised discharge date, and the gaps between all the dates should be plausible (unless that is what is being tested).

The "right to be forgotten" (see IRI's technical description of this ***here***) embodied in much privacy law (with some exceptions) is a particular problem, particularly for archives designed and implemented before privacy was an issue. You need to be able to find any PII for a particular person in such archives; you need to be able to delete it securely (and random access to tape archives, say, is notoriously expensive); you need to be sure that deleting one record doesn't corrupt the archive by removing embedded links etc.; and you need to know when the regulations let you ignore the right to be forgotten (and with what caveats and controls). In many cases, you will need expert advice. Some of which may be that "data swamps" (or even "data lakes") containing PII (and how would you know) are risky. You should probably have a policy of deleting data as soon as you can, as long as no-one is using it and the regulations allow it.

Privacy regulations can be quite sophisticated. Friedland points out that ***HIPAA*** (a US healthcare-oriented privacy regulation) compliance can require that you analyse "quasi-identifiers" (fields that don't identify a given person uniquely by themselves but can if you look at sufficiently many of them) and reject an anonymisation scheme if it doesn't score well enough. So IRI can score the risk of re-identification based on which identifiers (whether direct or indirect) are available and "tune" the anonymisation of quasi-identifiers so they are changed just enough to protect privacy adequately, without corrupting the information – it's all about risk management.

Friedland agrees that while HIPAA is pretty prescriptive, GDPR is less so. GDPR is not just a question of ticking a box, and you may find yourself explaining to the regulators just how your processes and procedures (and technology) actually protect privacy. This probably makes it harder to simply pay lip service to GDPR (at least, when the regulators come knocking), and it places greater demands on the flexibility of GDPR tools, but it does make GDPR less invasive, if you already implement good practice. It also means that if you have good policies and procedures in place, if you are unlucky

"HIPAA... can require that you analyse *"quasi-identifiers"* (fields that don't identify a given person uniquely by themselves but can if you look at sufficiently many of them) and reject an anonymisation scheme if it doesn't score well enough."

enough to experience, say, a data breach, you may well find that you incur smaller fines than you would if you had ignored GDPR altogether.

We also discussed the differing views of privacy in different areas of the world. The EU sees data privacy as a basic human right. This might be true also in California (which has state-level privacy laws) but large areas of the USA see something like GDPR as inimical to their business models and, basically, as just a barrier to trade. Nevertheless, despite cultural differences, everybody worries about the possible abuse of data, data theft and so on.

Why should you care about information privacy?

You should care, immediately, because penalties for non-compliance with information privacy laws are often severe: in the case of GDPR, up to €20,000,000 or 4% of the previous year's worldwide turnover, whichever is greater. However, we think that an even greater consequence, potentially, of non-compliance is reputation risk. A data breach is likely to get a lot of press coverage and makes your company look unprofessional, so not the sort of company one wants to do business with. At the same time, your competition may be promoting themselves as a better moral choice, the sort of company that takes care of its customers and looks after the privacy of their PII.

The fact that perhaps you got unlucky, and your competition didn't, is largely beside the point. Even so, if you are, say, GDPR-compliant and on the ball, you can tell a much better story in the press if you do happen to experience a data breach. Which is less likely anyway, as the process of instigating a privacy culture and putting in place information privacy policies and procedures, makes you less vulnerable, a less likely target for a successful attack.

There is also the issue that proactive compliance with information privacy law will help you convince the authorities that you are, indeed, making "best efforts" to comply and will address any shortcomings, which may well reduce any sanctions applied. Plus, you won't find yourself on any alleged list of "companies to make an example of" if the authorities ever need to underline the point that information privacy matters.

Finally, you should care about information privacy compliance because attaining it will encourage internal discipline and, in part, help you to become a better managed company that is trusted by your partners and customers. It will also reduce barriers to doing business with, say, the EU. Information privacy compliance is not just a cost of doing business, it is a positive benefit to the business, in that it helps to make the business a more trusted part of the commercial environment and more trusted by its customers.

"...you should care about information privacy compliance because attaining it will encourage internal discipline and, in part, help you to become a better managed company that is trusted by your partners and customers."

Information privacy, the bottom line

The bottom line is that information privacy is becoming important, not just from an individual point of view but also because protection of privacy can be a condition for trading information and because of the reputational and financial risks of failing to protect information.

Increasingly, also, data privacy laws have real teeth, with large fines expressed as an absolute limit or as a percentage of turnover, whichever is greater.

So, most firms are now taking information privacy very seriously (even if they aren't always implementing good practice very well). And, things are not standing still. The next information privacy issues are probably going to be around ChatGPT and the like. Do I want my PII to be picked up and used to train an advanced AI model? Even more seriously, do I want my PII used to train an AI model to target me and people like me for sales campaigns (or even fraud)? And what about the use of PII to facilitate the preparation of "deep fakes"; or the use of AI to de-anonymise information by looking at quasi-identifiers? Information privacy is not going away as a concern.

"The next information privacy issues are probably going to be around ChatGPT and the like. Do I want my PII to be picked up and used to train an advanced AI model? Even more seriously, do I want my PII used to train an AI model to target me and people like me for sales campaigns (or even fraud)?"

About the author

DAVID NORFOLK
Practice Leader:
Development & Governance

David Norfolk was working in the Research School of Chemistry at the Australian National University in the 1970s, when he discovered that computers could deliver misleading answers, even when programmed by very clever people. His ongoing interest in getting computers to deliver useful automation culminated in his joining Bloor in 2007 and taking on the development brief.

Development here refers to developing automated business outcomes, not just coding. It also covers the processes behind automation and the people issues associated with implementing it. He sees organisational maturity as a prerequisite for implementing effective (measured) process automation and ITIL as a useful framework for automated service delivery. He also looks after Collaboration and Business Process Management for Bloor, and takes a lively interest in the reinvention of the Mainframe as an Enterprise Server.

David has an honours degree in Chemistry, a graduate qualification in Computing, and is a Chartered IT Professional. He has a somewhat rusty NetWare 5 CNE certification and is a Member of the British Computer Society (he is on the committee of its Configuration Management Specialist Group).

He has worked in database administration (DBA) and operations research for the Australian Public Service in Canberra. David then worked for Bank of America and Swiss Bank Corporation in the UK, holding positions in DBA, systems development method and standards, internal control, network management, technology risk and even PC support. He was instrumental in introducing a formal systems development process for the Bank of America Global Banking product in Croydon.

In 1992 he started a new career as a professional writer and analyst. He is a past co-editor/co-owner) of Application Development Advisor and was associate editor for the launch of Register Developer. He helped organise the first London CMMI Made Practical conference in 2005 and has written for most of the major computer industry publications.

He runs his own company, David Rhys Enterprises Ltd, from his home in Chippenham, where he also indulges a keen interest in photography (he holds a Royal Photographic Society ARPS distinction).

Bloor overview

Technology is enabling rapid business evolution. The opportunities are immense but if you do not adapt then you will not survive. So in the age of Mutable business Evolution is Essential to your success.

We'll show you the future and help you deliver it.

Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability and impact.

We provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

For over 25 years, Bloor has assisted companies to intelligently evolve: by embracing technology to adjust their strategies and achieve the best possible outcomes. At Bloor, we will help you challenge assumptions to consistently improve and succeed.

Copyright and disclaimer

Bloor Research International Ltd
20–22 Wenlock Road
LONDON N1 7GU
United Kingdom

tel: **+44 (0)1494 291 992**
web: **www.Bloorresearch.com**
email: **info@Bloorresearch.com**