Privacy governance survey

The state of privacy management in Belgian organisations

January 2017

pwc lawsquare

Welcome

How are Belgian organisations performing when it comes to the protection of personal data? In November 2016, PwC Belgium and Law Square launched a privacy governance survey. The aim of this survey is to give insight into Belgian organisations' readiness for the upcoming General Data Protection Regulation (GDPR) and their level of maturity in dealing with the protection of personal data.

We'd like to thank the more than 120 respondents who completed this survey. They represented a great diversity of company sizes and sector representation. The respondents were mostly individuals involved in data privacy and security, including security officers, data protection officers, compliance officers, internal audit directors, HR managers, legal counsel and management board representatives.

We hope you find the information in this report insightful and valuable in helping you to further direct the GDPR project within your organisation. The information obtained through the survey has solely been used for the preparation of this report.

At your request, we are more than willing to further discuss the results of this survey in the context of your own organisation, or to facilitate the development of an action plan that suits the focus of your organisation.

Sincerely yours,

On behalf of
PwC Belgium

Pascal Tops
Partner

On behalf of
Law Square

Karin Winters
Managing Partner

Table of contents

Introduction

Digitalisation has fundamentally altered the workplace behaviour for companies and organisations. The protection of personal data plays an increasingly important role within companies and organisations. Technology enables them to collect and process a larger amount of personal data. At the same time, society and politics become more critical on the amount of personal data collected and processed.

What is the General Data Protection Regulation?

The objective of GDPR is to protect natural persons with regard to the processing of personal data and set out rules to the free movement of personal data. As from 25 May 2018, European as well as non-European organisations processing personal data of European citizens should apply the new General data Protection Regulation (GDPR). This regulation has a major impact on organisations' data protection policies, processes, governance and overall how personal data needs to be handled in business. They will have to implement the new rules and must be able to demonstrate that they are compliant with the new rules. In case of non-compliance, the GDPR introduced substantially higher (administrative) penalties of up to 4% of an organisation's global annual turnover or EUR 20 million, whichever is highest.

To be compliant with the GDPR, organisations must, among other things:

- Be in continuous control of where, when and how personal data is being processed (also in relation to data processors)
- Store compliance files (processing, governance structure and responsibilities)
- Appoint a data protection officer (for some organisations)
- Conduct data protection impact assessments (DPIA) and implement safeguards and controls accordingly
- Process personal data in line with the data protection principles set forward in the regulation, including the data protection by design/default principle
- Report personal data breaches to the competent authorities within 72 hours
- Provide more information on personal data breaches to data subjects

Objective of the privacy governance survey

Our privacy governance survey provides an overall insight into how Belgian organisations deal with privacy, why they believe it is important, what they are doing about it and how they deal with current and new data privacy regulations.

The results can be useful for you and your organisation:

- Better understanding of the nature and impact of new privacy legislation
- Assess relevant privacy risks
- Raising awareness

How to use the results for your own purposes?

Based on the overall picture as presented in this report, we recommend:

- To discuss the report and the recommendations with the privacy stakeholders within your organisation enabling them to define strategic directions
- To translate strategy into an action plan resulting in implementation of organisational, procedural and technical measures
- To evaluate the effectiveness of the implemented GDPR measures periodically

Summary

The General Data Protection Regulation (GDPR) will impact European as well as non-European organisations processing personal data of European citizens. It requires significant efforts from organisations to understand and comply with the GDPR. Organisations still have some time as the GDPR will apply as from 25 May 2018. To get insights into Belgian organisations' readiness for the GDPR and their level of maturity in dealing with the protection of personal data, PwC and Law Square conducted a survey at the end of 2016.

More than 120 respondents completed the survey. Overall the results indicate that a majority of the organisations is still working on its GDPR compliance or even still need to start. This applies to almost all aspects of the GDPR. Including doing a data protection impact assessment in order to identify potential gaps to be remediated. But also related to the implementation of appropriate procedures and measures, e.g. on the right for correction of personal data by the data subjects or on the timely disposal of personal data. Similarly, on the required data breach reporting towards the supervisory authority and the data subjects, we noted that only a small proportion of companies reported being ready for this.

The general awareness of staff involved in the processing of personal data still seems to be a point of attention. People are often described as being the weakest link in the security chain and hence there is a strong need for periodic awareness campaigns and trainings. Organisations should not neglect the risk exposure created by their own employees.

So far the GDPR seals and certifications did not get a lot of attention yet in the general debates around GDPR. Also the respondents also indicated not to know whether they might be useful for organisations. However, these seals and certifications can contribute to create trust and to demonstrate GDPR compliance.

Surprisingly two-thirds indicated to have already embedded the 'privacy by design' principle. Another interesting insight is that the organisations active in regulated sector seemed to be in a better shape with regards to GDPR readiness. This is likely because they already have more strict and mature procedures and controls in place in the areas of their daily operations, information security and compliance.

It will be interesting to see how these results will further evolve towards next year, when we plan to do a follow-up survey. Organisations might think that they still have sufficient time to take the necessary steps forward, as 25 May 2018 may seem a long way off. However, the complexity and the number of measures to be taken to comply with the GDPR should not be underestimated. Not only from a technical point of view but also due to the cross-departmental and territorial impact on organisations. The principles with regard to the processing of personal data and rules should be fully integrated in the governance framework and be embedded in policies, processes and controls. In addition, the sustainability of these GDPR related implemented measures should also be ensured.

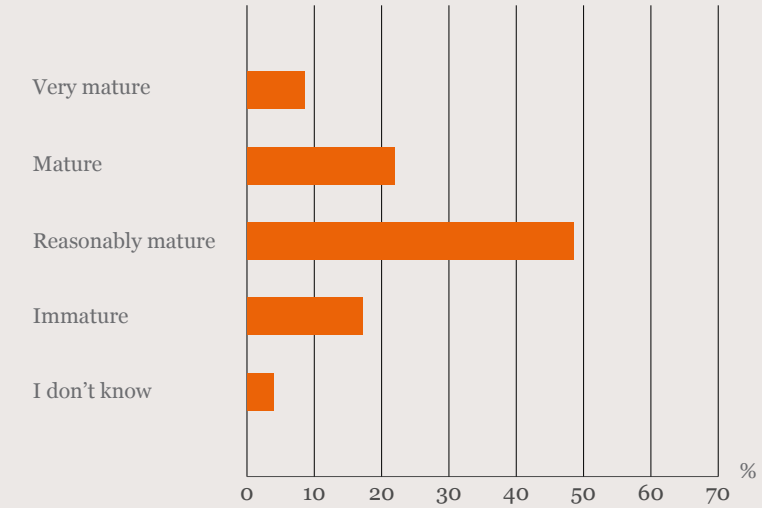
Key findings

A call-to-action for Belgian organisations

The GDPR strengthens the personal data protection requirements that companies will have to comply with by 25 May 2018. It is therefore important that organisations understand the interest of privacy and data protection and how this fits into their overall business strategy. Not complying with personal data regulation turns into a real risk for companies. If not compliant, fines can be up to 4% of the annual worldwide turnover or 20 million euro, whichever is the highest. For big organisations the fines can most likely go above the 20 million.

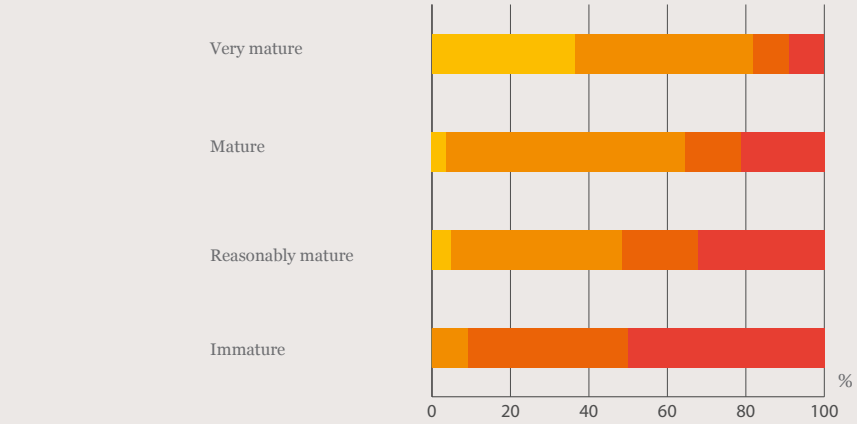
About 30% of all respondents declare that their organisation is already mature to very mature with regards to the processing of personal data in compliance with the GDPR. About 66% still have a lot of work to do to reach that same maturity level. This clearly indicates that Belgian organisations have still work ahead in becoming compliant by 25 May 2018.

In your opinion, how mature is the processing of personal data in your organisation?



However, the majority of organisations who consider themselves to be mature to very mature, are also still working on their GDPR implementation. A minority of them even still needs to start with the GDPR implementation or still have to identify the relevant changes in the privacy legislation. Almost all organisations in the immature category still have to start with their GDPR implementation based on the relevant changes identified or still have to start identifying those changes. In the remainder of this report, we will further highlight some detailed GDPR areas for which organisations still have to take further actions.

We are ready for the upcoming changes in privacy legislation (GDPR and the Belgian Act on Data Breaches), per maturity category



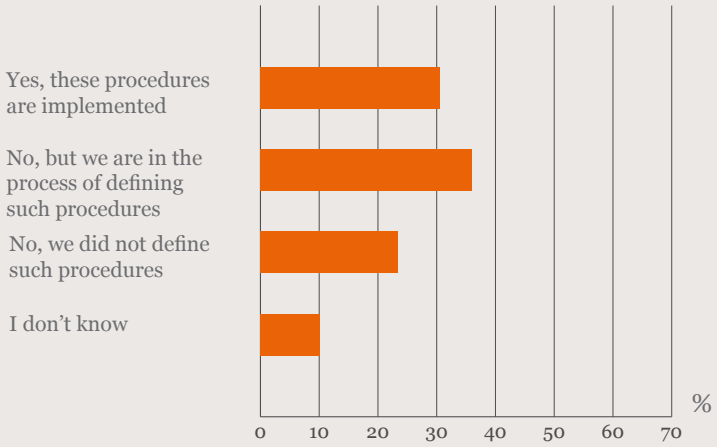
Only 30% already have procedures regarding transparency and personal data handling

The GDPR requires that any information and communication relating to the processing of personal data should be easily accessible and easy to understand, and that clear and plain language should be used. This is reflected as the 'transparency' principle. The regulation also requires that personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. The latter entails that the period for which the personal data are stored is limited to a strict minimum. This requires the controller to establish controls and procedures for the erasure of personal data or for a periodic review of this data. In addition, a data subject should also have the right to rectify his or her personal data.

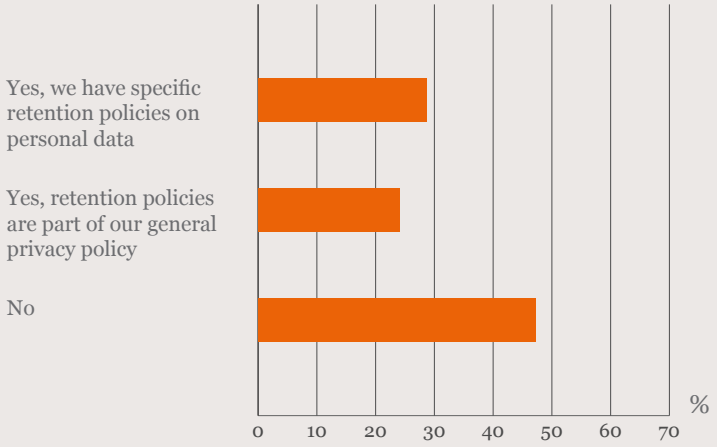
So far, only about 30 % of the organisations already implemented procedures regarding 'transparency' and the right for the correction of data by the data subjects. About 23% still have to start defining and implementing such procedures.

Related to the policies on the retention and disposal of personal data, the results show that about half of the respondents indicate that their organisation still have not implemented such policies.

Does your organisation have procedures regarding transparency and the right for correction of the data subjects?



Does your organisation have policies on retention and disposal of personal data?



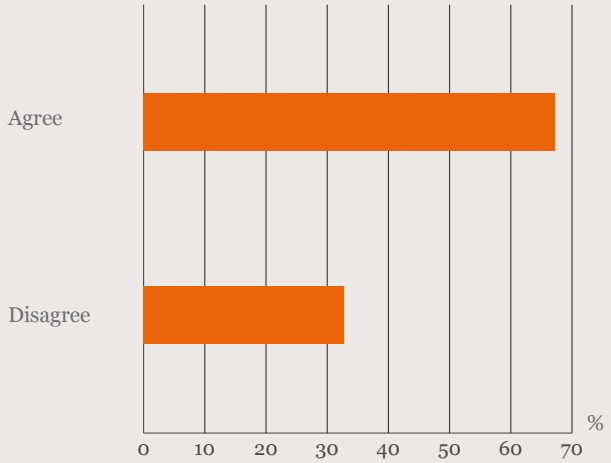
67% apply the ‘privacy by design’ principle

An important principle of the GDPR is the one related to ‘privacy by design’. The data controller must implement appropriate technical and organisational measures which are designed to implement data-protection principles in an effective manner or to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects.

These privacy measures must be in place both at the time of the determination of the means for processing and at the time of the processing itself. The survey results indicate that so far about 67% of the respondents indicate that their organisations already take the ‘privacy by design’ principle into account upon implementing new systems.

We regularly see that clients indeed assess the impact on data privacy at the start of a new project. However, often no specific measures are taken to ensure that ‘privacy by design’ is fully embedded in applications, services and products that are based on the processing of personal data. Organisations should for example take actions to integrate appropriate security features, to minimise the processing of personal data, to pseudonymise personal data as soon as possible or to enable data subjects to monitor the data processing.

Upon implementing new systems we always take into account privacy aspects and protection of personal data (Privacy by Design principle) in an early stage?

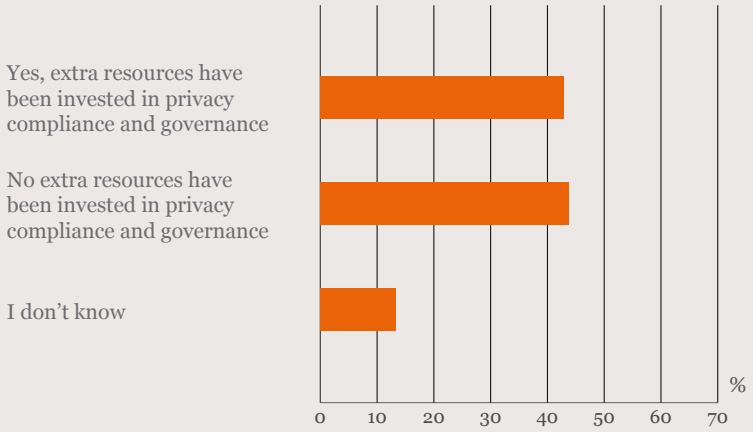


About 50% made extra investments in privacy compliance

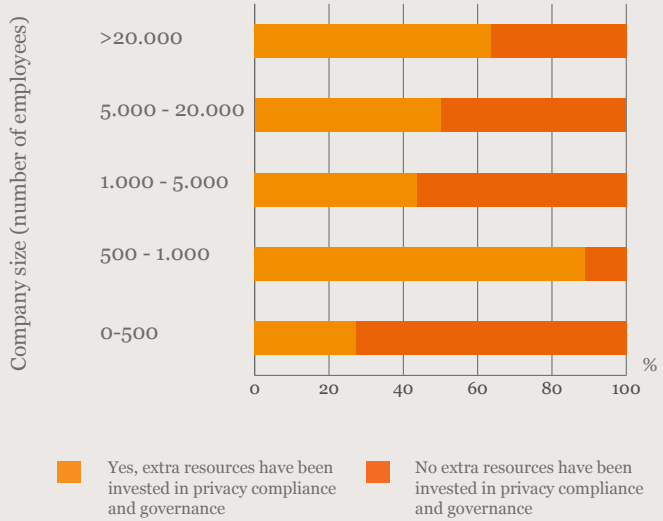
Our survey reveals that overall approximately half of all participants made extra investments in privacy compliance last year.

In looking deeper into the results and comparing the responses according to size and sector of the respondents, we found that, on average, the larger the company (based on number of employees), the more likely it is to have invested additional resources in privacy compliance and governance. There was however one exception to this rule, with no apparent explanation, for those respondents qualifying as companies with an employee range between 500-1000. In this category almost 90% of respondents indicated to have allocated extra resources in privacy compliance and governance.

Did your organisation make an extra investment in privacy compliance and governance last year?



Organisations that made an extra investment in privacy compliance and governance last year, according to their company size

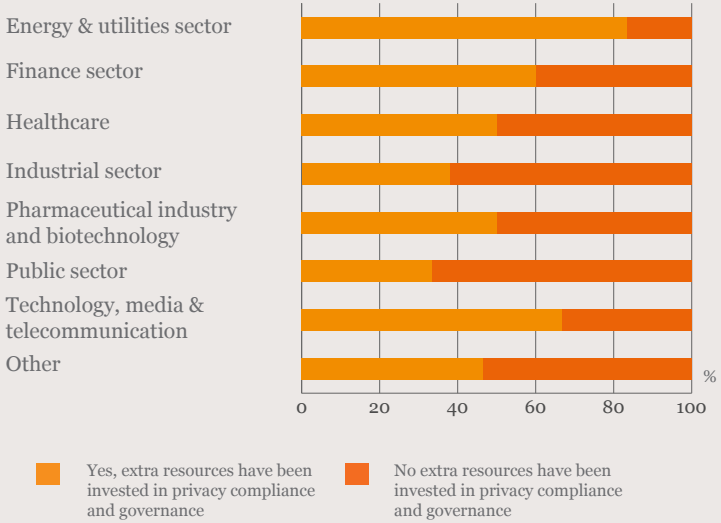


Larger companies tend to face an elevated risk resulting from non-compliance with privacy rules, or at least tend to show a lower risk appetite towards the resulting financial and reputational impact of non-compliance. As a result, they typically put in place a more structured approach towards risk and compliance, and allocate the necessary resources to compliance programmes. We expect data protection authorities will therefore express higher expectations in terms of compliance (programmes) from larger organisations than from smaller organisations.

With respect to smaller organisations we note that the GDPR originally provided several exceptions for small and medium-sized enterprises (taking into account the number of employees or the amount of data subjects on whom personal data was processed). Most of these exceptions did not live to see the light of day (except with respect to the obligation to maintain records of processing activities). It could be that our findings are merely a translation of the perception of such smaller organisations that the GDPR does still not apply to them or at least is less of a priority.

The sector in which the given organisation is active is also an important indicator when determining willingness to invest in privacy. Extra investment is particularly made in the finance, energy and technology sectors. The public sector entities show the lowest tendency to make such investments.

Organisations that made an extra investment in privacy compliance and governance last year, per sector



Only 38% have insight into their personal data flows and data processing

The GDPR requires that organisations are in continuous control of where, when and how personal data is being processed, also in relation to data processors.

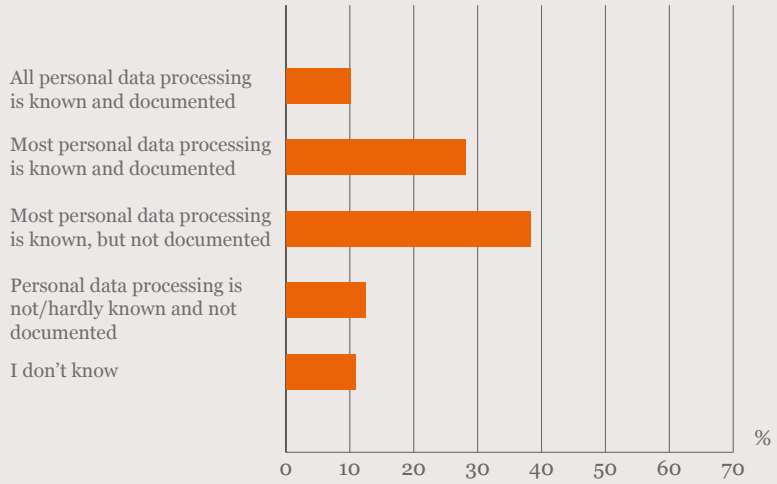
The survey results show that organisations have limited insight into their own personal data processing activities, which is worrying. Identifying data processing activities within organisations and maintaining related records is a mandatory requirement of the GDPR. However, we noted that:

- → Only 38% of the organisations state that most or all of their personal data processing is known and documented
- → 23% of the organisations do not know which personal data is sent to third parties

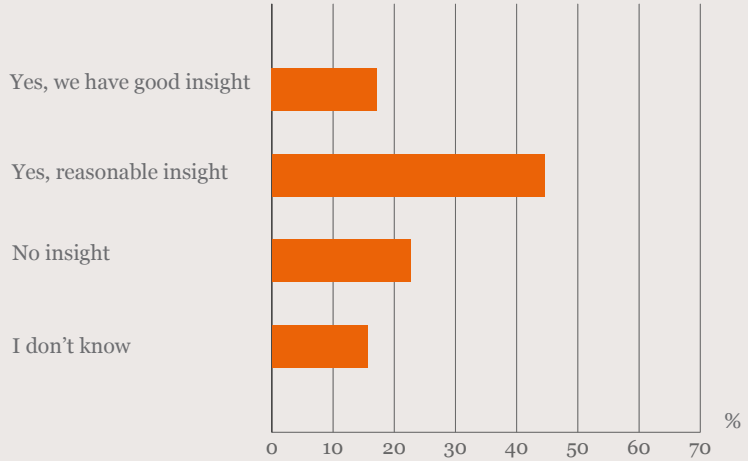
We acknowledge the challenge of identifying personal data flows throughout an organisation and its stakeholders. Before rushing into documenting data flows, we advise to define a process and toolset for the identification and documentation of personal data flows and, more importantly, for the maintenance of this documentation.

For organisations processing large amounts of personal data, we believe that an essential element in pursuing GDPR compliance is the implementation of a data governance function.

Does your organisation have a clear view which personal data are processed and is this documented?



Does your organisation, from a privacy perspective, have insight in personal data flows between your organisation and third parties (suppliers, customers, data processors)?



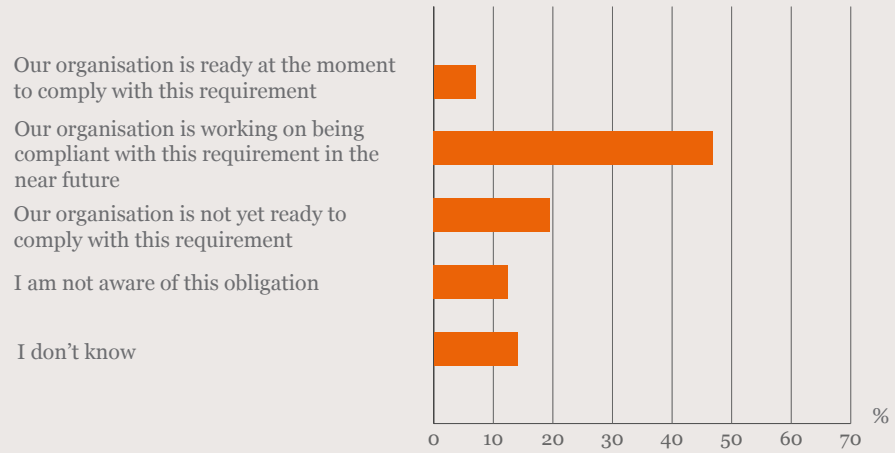
A large majority is not ready to report personal data breaches

The GDPR requires that the data controller notifies the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, about a personal data breach.

When it comes to data breach reporting, only a small proportion of companies reported being completely prepared to comply with this obligation. The overwhelming majority of participants are either unaware of the reporting obligation – and consequently, do not have any communication strategy when it comes to such reporting - or are currently unprepared to comply. A relatively small number of participants are in the process of ensuring compliance, however. Generally it can be stated that awareness of and ability to comply with the new regulation is significantly less than optimal.

Having an adequate communication plan is a key feature. Such communication plans are present at less than a third of all participants. However, some organisations that are relatively well-prepared for the new GDPR rules do not yet have an adequate plan for their communication towards the data protection authority and/or the data subjects. It seems like communication plans are frequently treated as a low-priority issue. In addition, the survey results also show that less than half (47%) of the organisations is compliant with the statutory obligation to keep a central record of data breaches.

Is your organisation well-prepared to notify, as of 25 May 2018, data breaches without delay to the supervisory authority and under certain conditions to the data subjects involved?



50% have already performed a data protection impact assessment

The GDPR requires a data protection impact assessment (DPIA) to be performed where processing operations are likely to result in a high risk to the rights and freedom of natural persons.

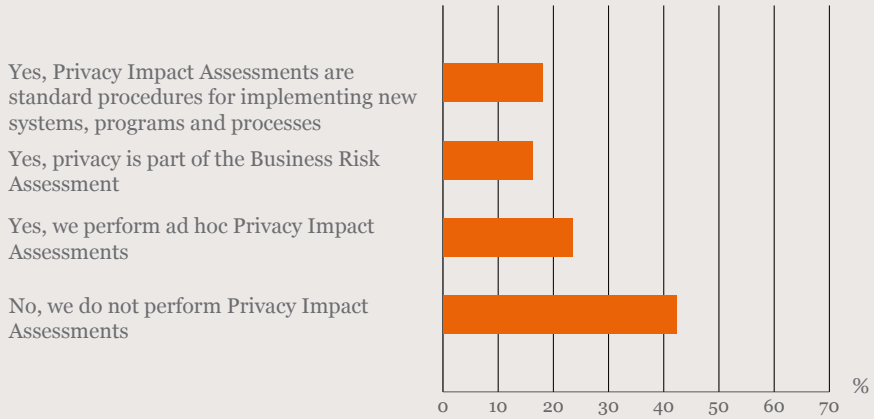
Although not always required, performing a DPIA allows organisations to get a good view on the risks related to their personal data processing activities. It enables the identification of problems at an early stage so that they can be addressed in an efficient and cost effective way.

Based on the results of the DPIA, organisations will have the necessary input to start prioritising, addressing and mitigating the identified risks. It will help to assess their current situation and to get a clear view on gaps that must be remediated.

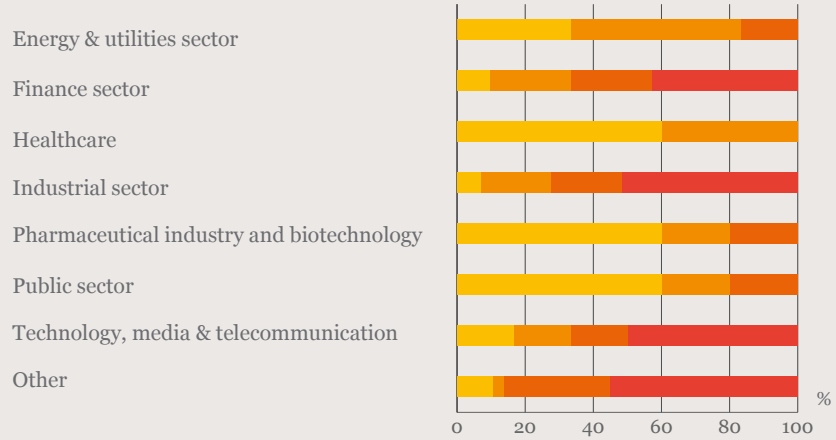
The DPIA should also include an evaluation of the design and the effectiveness of the internal controls in place to mitigate the privacy related risks. Processes and internal controls are a crucial element of the governance framework to ensure that organisations not only become GDPR compliant but also remain GDPR compliant in the future. Hence, it is valuable to perform a DPIA or do an update, for example each time a new project is started entailing the processing of personal data.

The results from the survey show that already more than half of the respondents have performed a DPIA. In the sector comparison, in particular the pharmaceutical companies stand out, as most of them seem to already have performed these assessments. We think this is due to the high volume of sensitive personal data processed as well as the demanding regulatory requirements.

Does your organisation conduct risk analyses (e.g. Privacy Impact Assessments) concerning personal data processing?



Organisations conducting risk analyses (e.g. Privacy Impact Assessments) concerning personal data processing, per sector



- Yes, Privacy Impact Assessments are standard procedures for implementing new systems, programs and processes
- Yes, privacy is part of the Business Risk Assessment
- Yes, we perform ad hoc Privacy Impact Assessments
- No, we do not perform Privacy Impact Assessments

Are employees sufficiently aware of privacy?

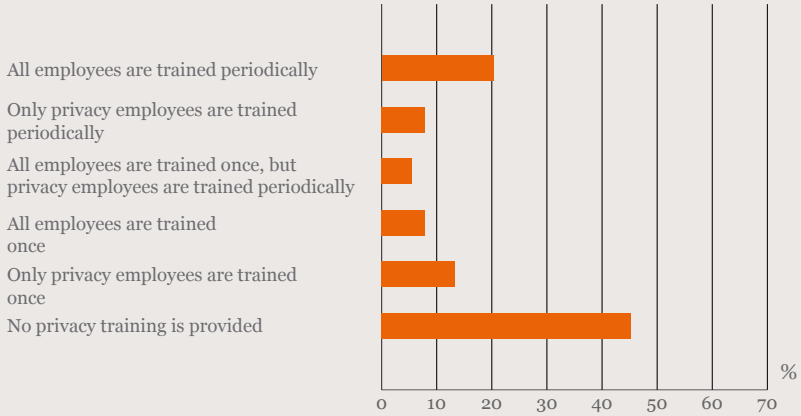
The GDPR states that the data protection officer or any other person in charge of the compliance with this regulation shall create awareness and organise trainings of staff involved in processing operations and the related audits.

About 45% of the respondents indicate that no privacy training is provided and another 35% indicate that not all their employees are trained periodically.

People are often the weakest link in the security chain. Organisations should not neglect the risk exposure created by their own employees. Hence, privacy training and awareness should be in place for educating employees, and to brief them about evolving privacy expectations and the relevant privacy issues in their organisation. These trainings should be provided on a regular basis. Training is an essential building block for the well functioning of a GDPR governance programme.

To support these trainings and awareness programmes, organisations should set the tone at the top. Topics to be covered as part of the awareness and training programmes should include among others the framework for managing privacy and compliance, the data-use governance framework and the data protection impact assessment approach.

How are employees in your organisation trained in the field of privacy?



About 42% have no opinion about the value of data protection seals and certifications

The GDPR regulation foresees the possibility of the use of certifications, seals and marks for the purpose of demonstrating compliance with the regulation of processing operations by controllers and processors. We expect that implementing acts will be issued by the European Commission to further clarify the technical standards for certification mechanisms and data protection seals and marks. In addition, the criteria applicable to the certification still have to be elaborated by the supervisory authority or by the European Data Protection Board.

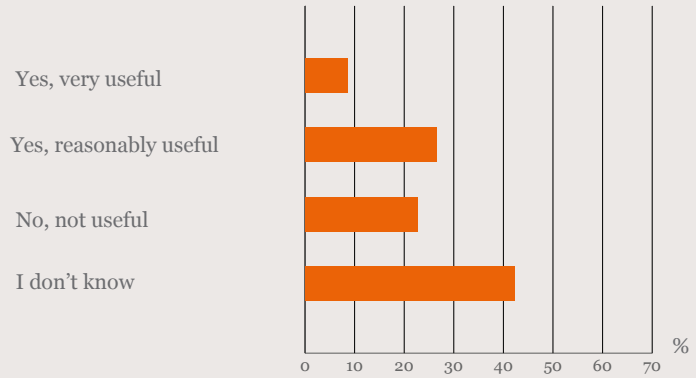
The survey results show that about 42% of the respondents do not know whether a GDPR seal might be useful for their organisation. However, we think that these certification mechanisms are indispensable. Organisations might want to show that they are serious about the privacy of their clients' personal data. Hence, a seal can be a solution to demonstrate compliance with GDPR.

Organisations outsourcing part of the personal data processing to third parties, should also be interested. It is important that organisations perform the necessary oversight of these third parties, their control environments and their adherence to GDPR requirements. A controller or processor can be held liable for the entire damage caused to data subjects, even when the processing was (partly) outsourced. Hence, organisations have to put in place a proper third-party risk management process to adequately manage their risks related to outsourcing.

This entails that organisations processing personal data for multiple organisations should definitely consider becoming certified in order to demonstrate GDPR compliance to their clients. This among others to avoid having to undergo a GDPR audit by each of their clients.

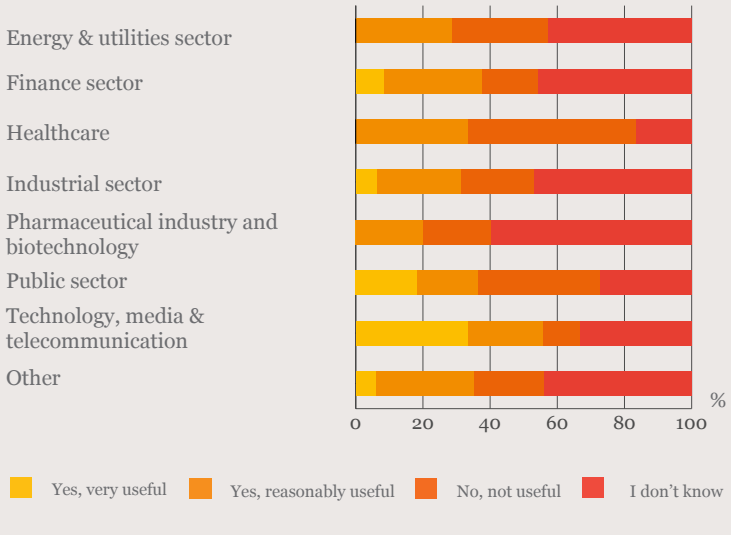
Several general types of audit certification are common on the market, including ISAE 3402, ISAE 3000 but also ISO type certifications. However, certifications should provide sufficient assurance towards clients on compliance with GDPR requirements.

The GDPR makes it possible for organisations to obtain a European Data Privacy Protection Seal. In your opinion, is it useful for your organisation to obtain a European Data Privacy Protection Seal?



It is also interesting to see that in particular the technology, media and telecom sector have the highest scores on the usefulness of GDPR certifications. This is typically a sector doing lots of data retention or processing for many organisations, e.g. data centre providers.

Usefulness of privacy certifications and seals, per sector



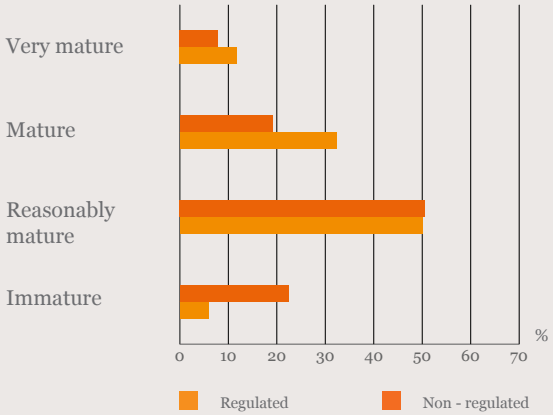
The GDPR does not differentiate between regulated and non-regulated sectors

Depending on the specific business and the sector, GDPR will be approached differently based on among others the organisational culture, priorities and risk appetite. In addition, certain sectors are already more regulated than others and consequently have more strict and mature procedures and controls in place in the areas of daily operations, information security and compliance. Hence we compared the survey results of regulated companies with those of less regulated ones. We considered the finance, healthcare and pharmaceutical sectors as the more regulated ones.

The survey results show that:

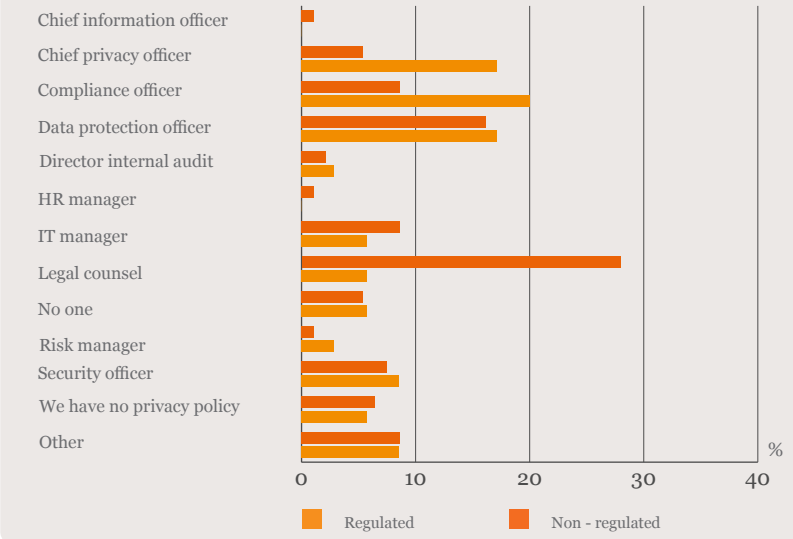
- About 44% of the respondents in the regulated sectors consider themselves already (very) mature w.r.t. the processing of personal data, while this is only about 27% in the non-regulated sectors. Also remarkable is that still about 23% of the respondents within the non-regulated sectors consider their organisations as immature in this respect, while the deadline to be compliant is approaching rapidly.

In your opinion, how mature is the processing of personal data in your organisation?



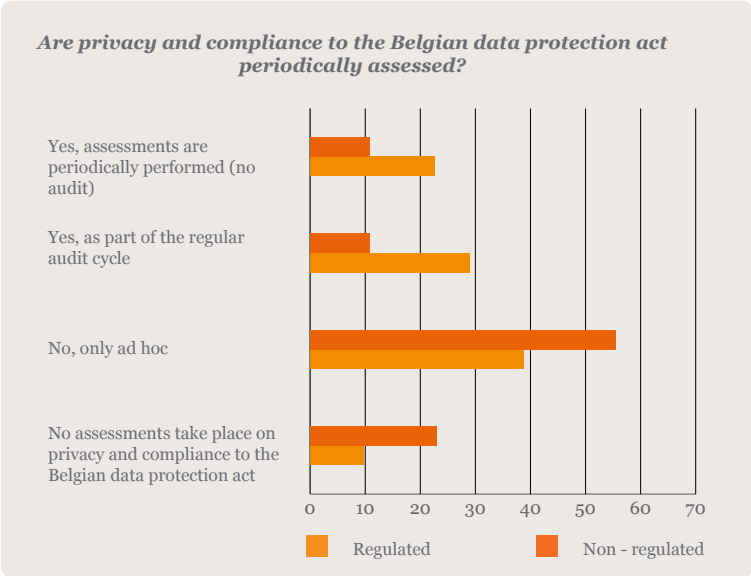
- Within the non-regulated sectors the lead on privacy is typically taken by the legal team or the data protection officer. In the regulated sectors, the responsibility typically is assigned to the compliance officer, chief privacy officer or data protection officer. This clearly demonstrates that regulated companies acknowledge that privacy and GDPR are not primarily a legal issue but rather something that has to be owned and driven transversally in the organisation.

Who is currently responsible for the implementation of your organisation's privacy policy?



→ About 52% of the respondents in the regulated sectors indicate they periodically assess compliance with the Belgian Data Protection Act, while this is only 22% for the non-regulated sectors. In general, further efforts will be required. Doing regular assessments will help organisations to identify the gaps in their privacy protection measures. Only when they become aware of these gaps, they will be able to take corrective actions.

→ The regulated sectors are already doing better on periodically providing privacy trainings to their employees (about 37%). In the non-regulated sectors no privacy related training is provided at all for about 52% of the respondents. As mentioned before, creating awareness about the privacy risks and mitigating controls will be a key element to be able to remain compliant with privacy requirements.



Although the regulated sectors seem to be in better shape as regards GDPR readiness, we see that both sectors still have to take further measures in order to become GDPR compliant. However, the GDPR does not make a distinction between regulated and non-regulated sectors. The same rules apply to both sectors.

Our GDPR journey

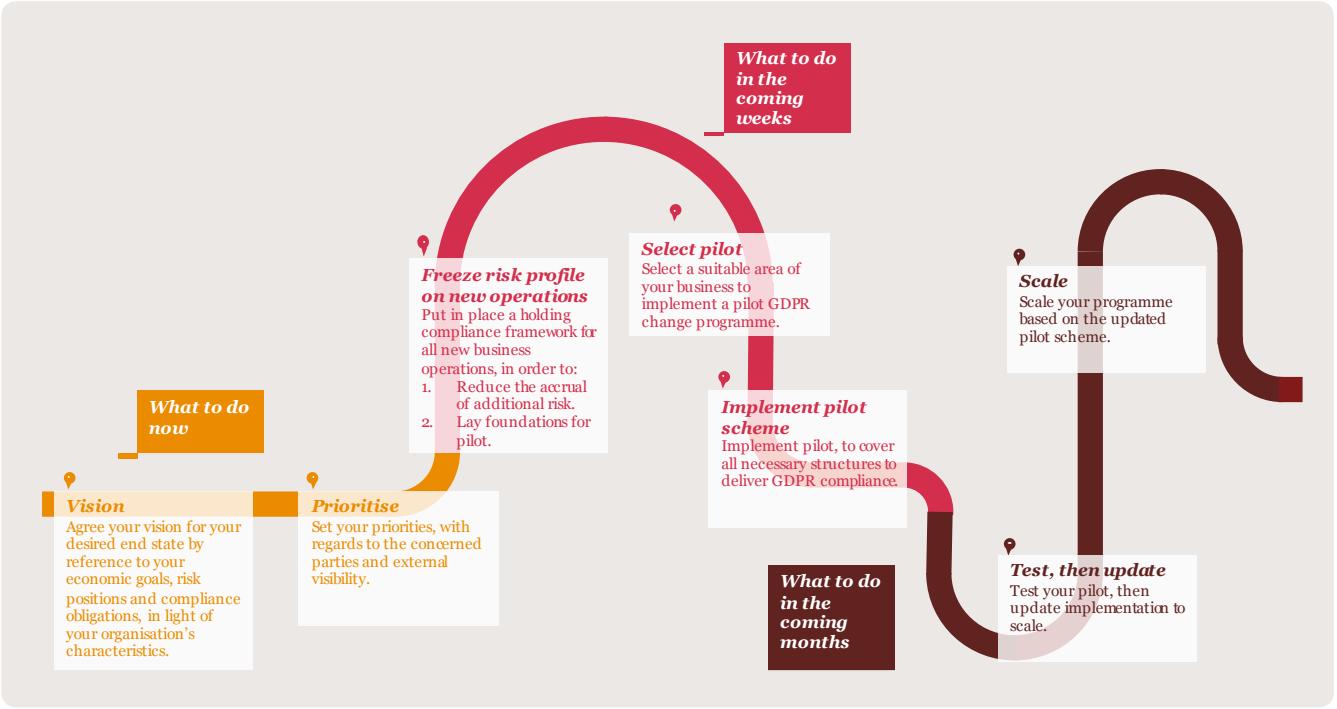
Our GDPR journey is optimised for economic goals, risk and compliance, and your special characteristics.

If you strip the GDPR to its essence, you will find that it contains a new legislative compliance journey, which many organisations are following in a truly linear sense. A problem is that the GDPR does not provide organisations with any insights into prioritisation.

There is a real risk that organisations that follow this linear path will simply end up spending a huge amount of time on e.g. data mapping, rather than getting on with dealing with the things that matter the most to them and to the parties concerned (i.e. customers, data protection authorities, employees, privacy advocates, etc.).

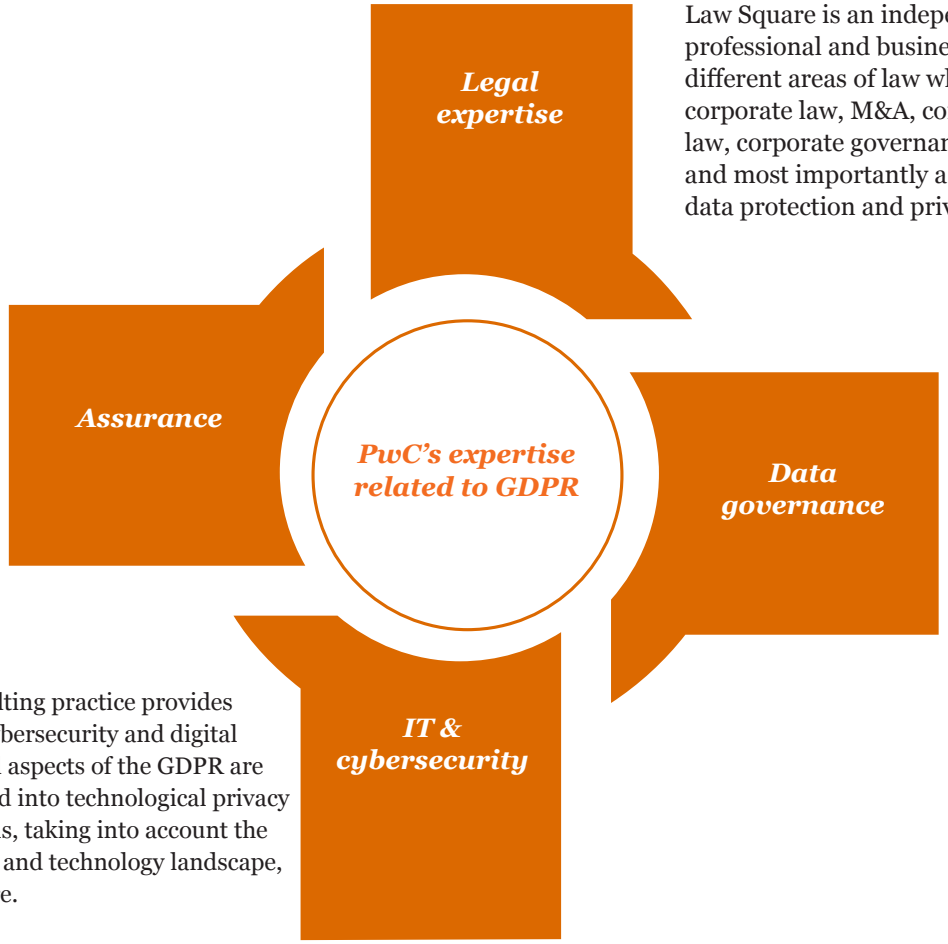
Organisations should consider their economical goals and risk appetite in conjunction with their compliance obligations to define their GDPR journey.

We have created a GDPR journey which allows you to build a prioritised roadmap, keeping your desired end state in mind, which transforms your current organisation into a GDPR-ready organisation. This roadmap puts in place a compliance framework and implements projects that are scaled up throughout your organisation and foresees continuous improvement of this framework.



PwC's expertise related to GDPR

Deriving synergies from our multidisciplinary strengths



Law Square is an independent law firm providing professional and business-oriented advice in different areas of law which include among others corporate law, M&A, commercial and contract law, corporate governance, corporate compliance and most importantly a dedicated team of legal data protection and privacy professionals.

PwC's Risk Assurance team assist clients in assessing privacy risk and compliance, establishing a governance framework and providing support to compliance functions. They also provide assurance through privacy and internal audit services, and issue third party assurance reports or certification.

An essential element in pursuing GDPR compliance is a mature data governance function. This makes it possible to locate personal data used throughout all business processes, impose policies and processes governing data collection, processing, archiving and deletion, embed privacy within the existing data security classification scheme, and help assure data quality within all processes.

PwC's Technology Consulting practice provides services in the areas of cybersecurity and digital transformation. The legal aspects of the GDPR are interpreted and translated into technological privacy and cybersecurity controls, taking into account the impact on the existing IT and technology landscape, and organisational culture.

Contact

Would you like to have more information about our privacy governance survey and about how we could help your organisation?

Karin Winters
Managing Partner, Law Square
t. 02 710 74 04
m. 0476 602 694
karin.winters@lawsquare.be

Carolyne Vande Vorst
Senior Managing Associate, Law Square
t. 02 710 91 28
m. 0476 275 129
carolyne.vande.vorst@lawsquare.be

Pascal Tops
Partner Risk Assurance, PwC
t. 02 710 33 56
m. 0473 910 368
pascal.tops@be.pwc.com

Bart Kuipers
Director Risk Assurance, PwC
t. 02 710 97 54
m. 0475 59 00 70
bart.kuipers@be.pwc.com

Filip De Wolf
Partner Technology Consulting, PwC
t. 02 710 42 51
m. 0478 484 329
filip.de.wolf@be.pwc.com

Jan De Meyer
Director Technology Consulting, PwC
t. 02 710 42 86
m. 0476 393 204
jan.de.meyer@be.pwc.com

www.pwc.be

www.lawsquare.be