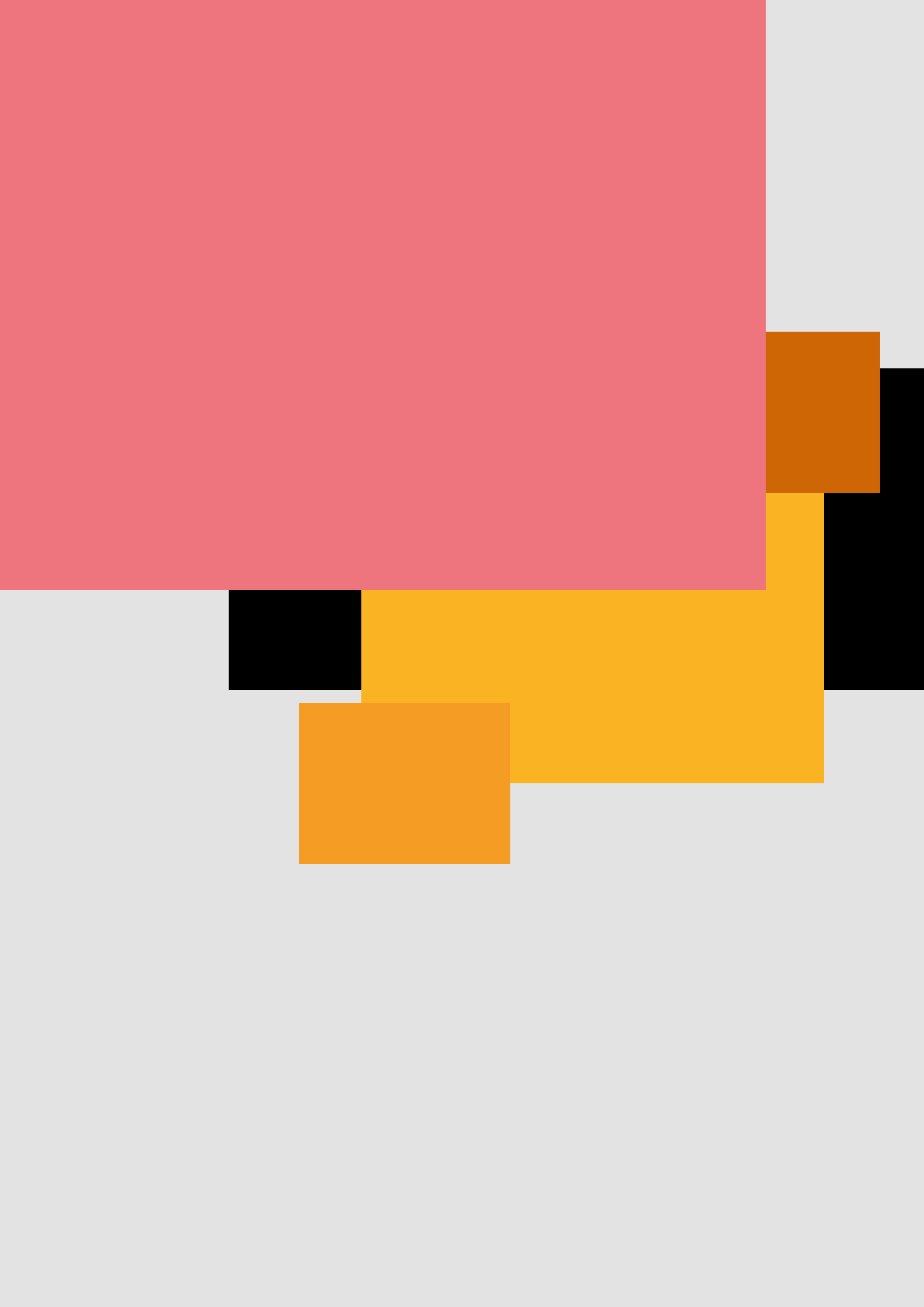
December 2018

General Data Protection Regulation

Luxembourg market status: Smooth Sailing or Hot Water?

pwc

www.pwc.lu/GDPR



Foreword

It has been over six months that the EU's General Data Protection Regulation ("GDPR") came into application on 25 May 2018. After a feverish rush for compliance that overtook many businesses, a period of relative calm followed, anticipating the first controls of the local supervisory body, the Commission Nationale pour la Protection des Données ("CNPD").

We aimed at understanding the Luxembourg market's reactions to the Regulation. In this respect, a survey of 15 questions addressing the GDPR readiness was sent to Luxembourg actors from different industries, focusing on various GDPR requirements.

In this report, we put forward the results of our research, shedding more light on the current data protection practices in Luxembourg as well as a general overview how organisations in Luxembourg cope with the key GDPR principles.

I would like to personally thank all 130 respondents for taking the time to share their thoughts.

Frédéric Vonner
GDPR and Privacy Leader

Executive Summary

> Respondents seem to be relatively confident regarding their compliance

Sailing into a deep and turbulent ocean of technological and business developments to maintain a competitive edge requires significant knowledge in several fields, now including the GDPR, in order to avoid being caught up in the pitfalls of bad data protection governance.

In a nutshell, the GDPR, being a big change maker in the data protection landscape, induces new requirements and constraints for the different services and departments within entities, regardless of their respective industries. In this report, we split the industries in three groups, namely the financial services companies, the operational companies and a last section englobing public, para-public, supra-national institutions, as well as all other entities, not within the industry sectors mentioned above.

The results of the survey reveal to what extent Luxembourg players are organised and practically, how they apprehend the new measures imposed by the GDPR. The topics included in the survey are the risk approach, the appointment of a Data Protection Officer ("DPO"), the management of retention periods, the management of data subject requests and breaches, the use of (new) security measures and the desire to become CARPA-certified in the future.

Nearly 90% of the respondents, led by those from the financial sector in terms of maturity, consider themselves as close to or actually GDPR-ready, by having implemented most of the GDPR requirements already, or implementing them in the near future. Throughout all industries, mapping the personal data processed has been seen as the biggest challenge in the GDPR compliance journey.

What immediately draws attention when looking at the survey results, is the contrast between the self-assessment of GDPR-compliance (half of the respondents considering that they fulfill the majority of the GDPR requirements and an additional 40% consider that they will fulfill these requirements in the near future) and the actual performance of risk assessments, whether it comes to assessing the risks for data subjects or the data processing activities themselves. Indeed, half of the respondents state that they have identified the risks for data subjects, without having mitigated them. The majority of the respondents state that they have not conducted a Data Protection Impact Assessment, while another significant part of them responded that they have not put this action on their agenda.

Another interesting learning from the survey lies in the fact that almost three quarters of the respondents are self-assured they have not faced a personal data breach, irrelevant whether such breach is to be reported to the CNPD or not. This raises questions, whether these entities have not been able to identify data breaches rather than not being subject to one, or whether the understanding of what makes a breach reportable to the authority is properly understood.

The survey results also suggest that drafting procedures regarding the transparency of processing was one of the first priorities of the respondents, as the vast majority of these entities have implemented such a procedure.

Whether or not this has influenced the number of data subject requests is unclear, however it seems that one of the goals of the GDPR, giving people more control over their data, has been achieved, as roughly a third of the survey respondents have had to deal with at least one data subject request.

Overall, the survey results suggest that respondents seem to be relatively confident regarding their compliance with the GDPR. However only time will tell whether the GDPR-compliance journey has truly been smooth sailing, or more focus should have been put to the assessment of risks related to personal data and the review of IT systems, suggesting hot waters ahead.

1

To what level is your organisation ready to comply with the GDPR?

After six months of the GDPR being in force, nearly 50% of the respondents state they have implemented the majority of the requirements and changes in order to be compliant with this Regulation focusing on Data Privacy. The remainder of the respondents have acknowledged that the GDPR is something on their action plan including 40% of the respondents indicating that they have started to implement certain elements, however still have to focus on certain important measures to implement. Once these remaining 40% finalise the implementation, this would suggest that 90% of companies in Luxembourg would feel compliant with the GDPR. The remaining 10% indicate they have had other priorities, but in the majority of cases, have started to plan the implementation of their GDPR compliance project.
The survey results show that the financial sector is slightly ahead in terms of GDPR-readiness compared to the other sectors. Interestingly enough, almost 9% of the respondents within the non-financial services have not yet decided on a GDPR strategy nor have started with the implementation.
When looking at the company in terms of employee number, 69% of the largest companies have indicated that they are GDPR-ready, whereas it is in the smaller companies that the level of readiness appears to be the lowest.

Table 1.1: Split by company size (number of employees)

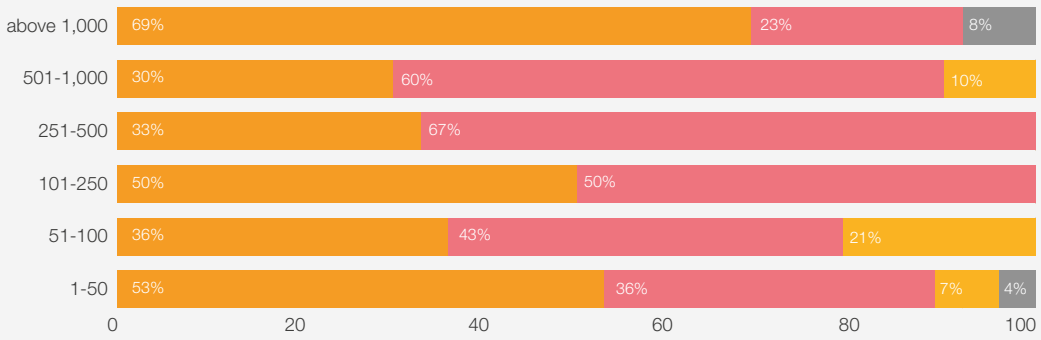
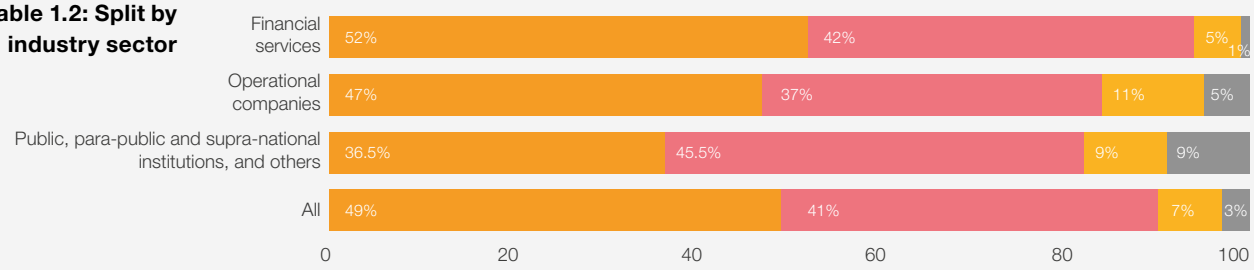


Table 1.2: Split by industry sector



- We have already implemented most of the requirements and changes of the GDPR within our organisation
- We have put in place certain changes and measures corresponding to the GDPR requirements, however we still have other important measures to implement
- We have started to plan the implementation of the GDPR project within our organisation, but no overall strategy has been decided
- We are aware of the GDPR, however we had other priorities for the moment or we assume it's not relevant to us, therefore we haven't started planning the GDPR project

2

Have you identified the main risk factors for the data subjects when it comes to personal data within your company?

A clear link can be seen between the level of GDPR-readiness and the identification of the main risk factors for the data subjects as well as their mitigation, as almost 50% of the respondents indicate they have identified and mitigated the risks. Roughly, 15% of respondents under 100 employees have not yet identified the risk factors for the data subjects compared to the remainder, who have indicated they have identified the risks, but in more than half of these cases, have not yet mitigated them.
As the GDPR is a regulation focusing on the protection of personal data by taking into account the risk for the individuals, we would have expected these numbers to be slightly higher for the entire spectrum of organisations, regardless of their sector or size.

Table 2.1: Split by company size (number of employees)

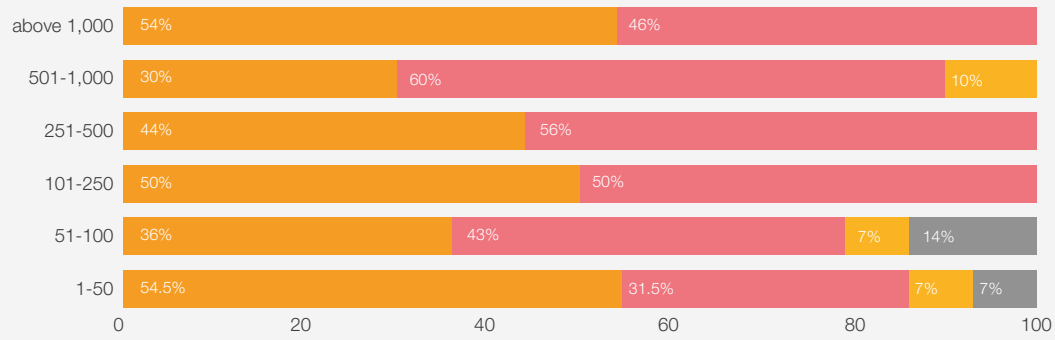
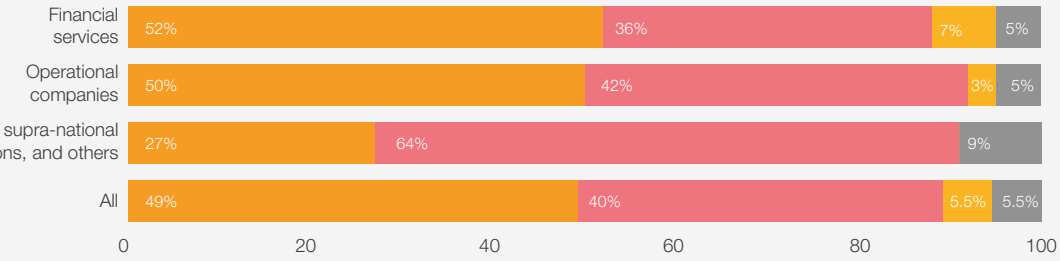


Table 2.2: Split by industry sector



- Yes and we have mitigated the risks
- Yes, the risks are identified but we have not yet mitigated the risks
- No, we did the analysis and have not identified any risk factors
- No, we have not started this analysis yet

3

What are/were the biggest challenges in the implementation of the GDPR measures?

Approximately two thirds of the respondents have indicated that the mapping of all personal data processing activities was one of the biggest challenges during their GDPR implementation project. Lack of staff availability was ranked second, closely followed by complex technological measures, both being identified as one of the biggest challenges by around 40% of the survey respondents. 40% of the respondents of entities under 50 employees have indicated that one of the biggest challenges was not only the mapping, but also the legal comprehension of the GDPR.

Table 3.1: Split by company size (number of employees)

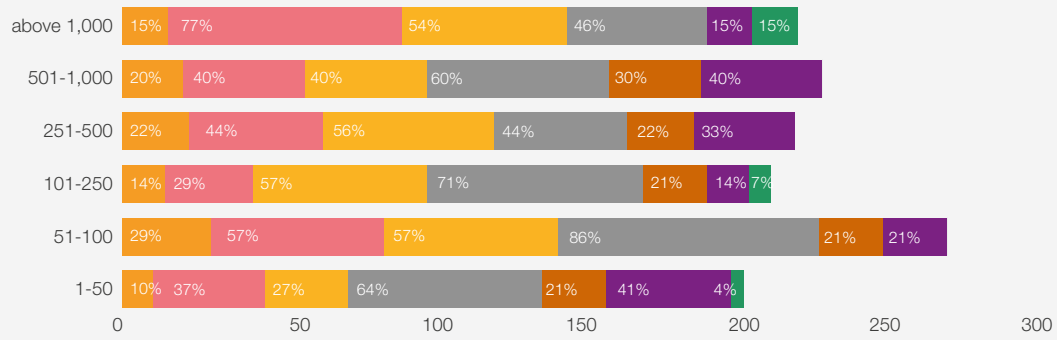
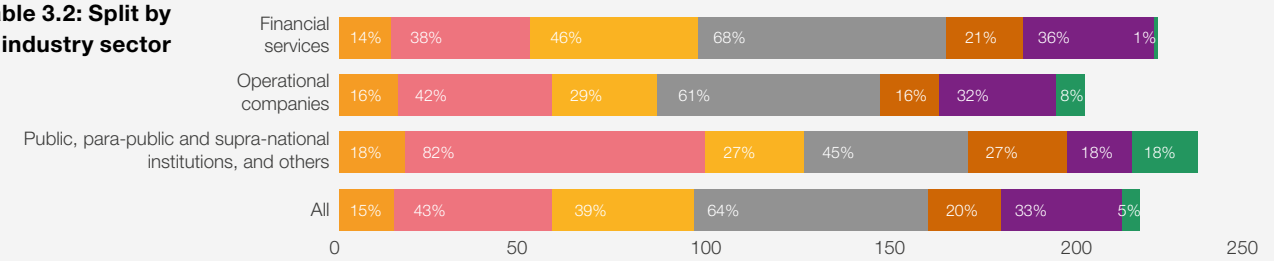


Table 3.2: Split by industry sector



- Financial expenditures
- Staff availability
- Complex technological measures
- Mapping all personal data processing activities
- Enabling data subjects to exercise their rights
- Legal comprehension
- Other

4

Has your organisation defined and documented retention periods?

Taking into consideration that nearly 90% of the survey respondents consider themselves as GDPR "ready" or "partially ready", the fact that a quarter of the organisations have not yet defined retention periods for personal data suggests that other GDPR measures have had priority over the enforcement of proper retention periods. The remaining majority of respondents have defined retention periods; however, their enforcement remains a pain point throughout the industry sectors.
The survey results show that the bigger the organisation in terms of employee numbers, the higher the probability the retention periods have been defined.

Table 4.1: Split by company size (number of employees)

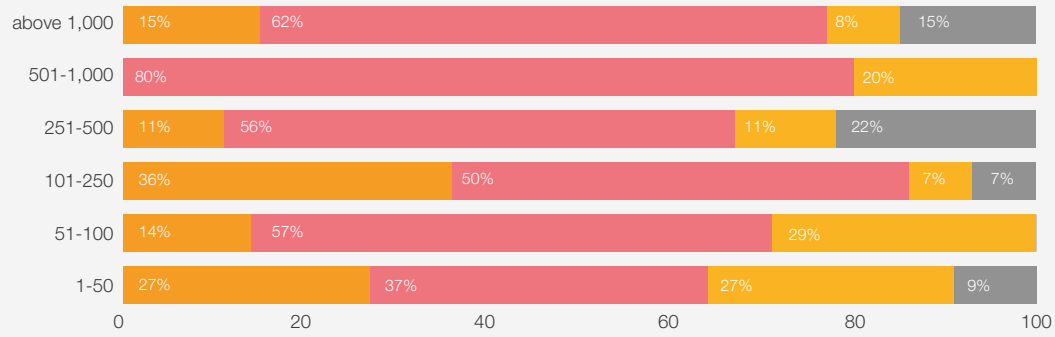
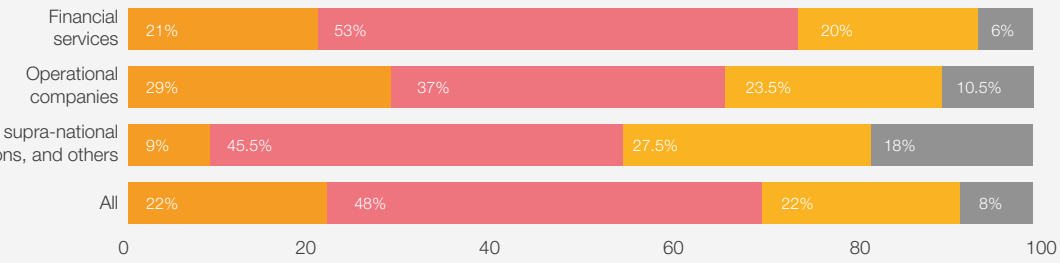


Table 4.2: Split by industry sector



- Yes, retention periods have been defined in our register of personal data processing and deletion is systematic following personal data maturity
- Yes, retention periods have been defined in our register of personal data processing; yet, we still need to enforce them
- No, retention periods have not been defined in our register of personal data processing, however personal data is deleted on an ad hoc basis
- No, retention periods have not been defined and we do not delete personal data

5

Have you analysed the level of risk of individual personal data processing activities and conducted a Data Protection Impact Assessment (DPIA)?

The risk assessment is the basis for any GDPR project and we have seen that nearly 90% of the respondents have identified the risks for the data subjects. Therefore seeing that 60% of the organisations have not conducted a DPIA assessment is rather surprising. Even more surprisingly, nearly 10% of respondents have highlighted that they have not conducted a risk analysis and do not plan to do so, which would suggest that their compliance with the GDPR is not a topic of the highest importance for them now.

Table 5.1: Split by company size (number of employees)

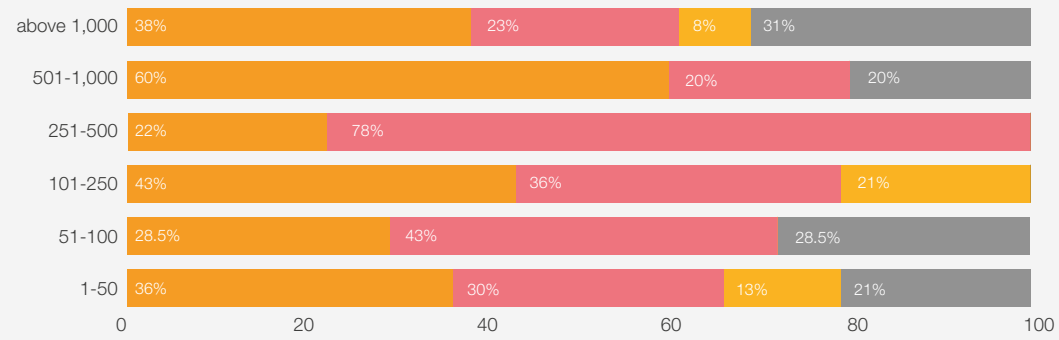
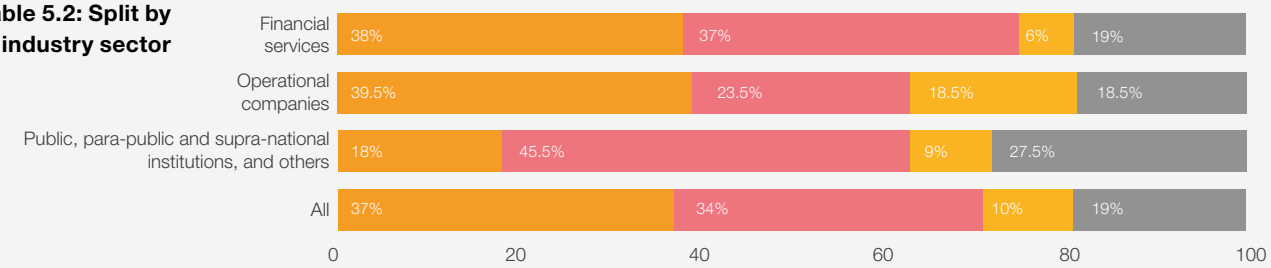


Table 5.2: Split by industry sector



- Yes, we have analysed all our personal data processing activities and we have conducted a DPIA on the identified processing
- Yes, we have analysed all our personal data processing activities; however we have not conducted the necessary or all DPIA yet
- We have not conducted the risk analysis and do not plan to do so
- We have not conducted the risk analysis yet, but will do so in the near future

6

Do you take GDPR-related risks into account for your internal audit plan?

Half of the respondents have included the GDPR within their internal audit plan and plan to conduct a GDPR audit either this, or next year. Around 20% of the respondents indicated they do not have an internal audit department and an additional 20% having an internal audit department, have not updated the audit plan with GDPR-related risks.

Table 6.1: Split by company size (number of employees)

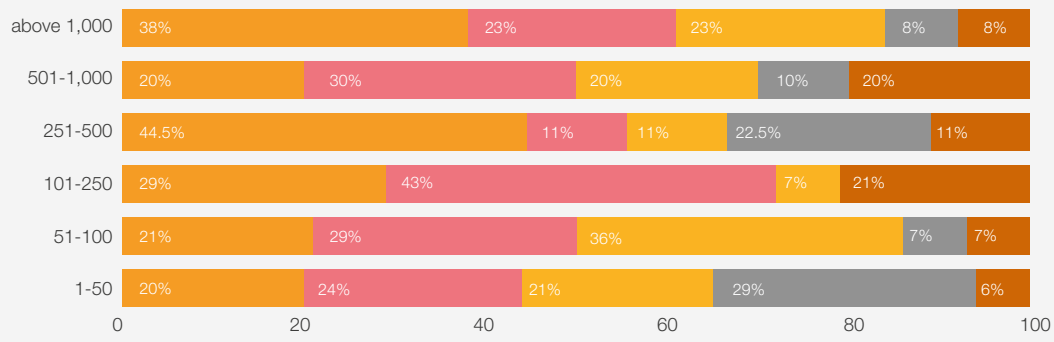
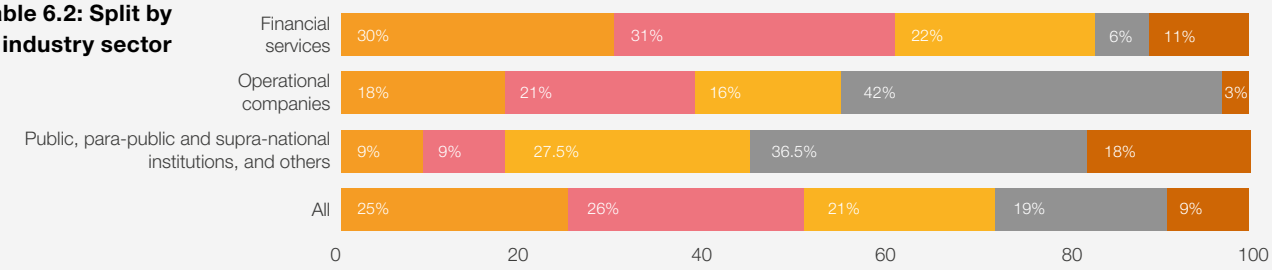


Table 6.2: Split by industry sector



- Yes, we have updated our internal audit plan to take into account GDPR-related risks and we will conduct such audit this year
- Yes, we have updated our internal audit plan to take into account GDPR-related risks. Yet, we will not conduct such audit this year
- No, we have not updated our internal audit plan with GDPR-related risks
- We do not have an internal audit department
- I do not know

7

How do you make sure your critical business partners, incl. data processors, are compliant with the GDPR?

More than a quarter of the respondents have indicated that they have put the burden of contractual updates on their counterparts and expect their critical business partners to approach them with proposed contractual updates.
More than half of the organisations have faith in the GDPR-readiness of their counterparts and have taken the time to update the mutual contractual agreements. 8% of respondents do not consider updating their contracts with critical business counterparts as relevant, therefore do not plan to do so.

Table 7.1: Split by company size (number of employees)

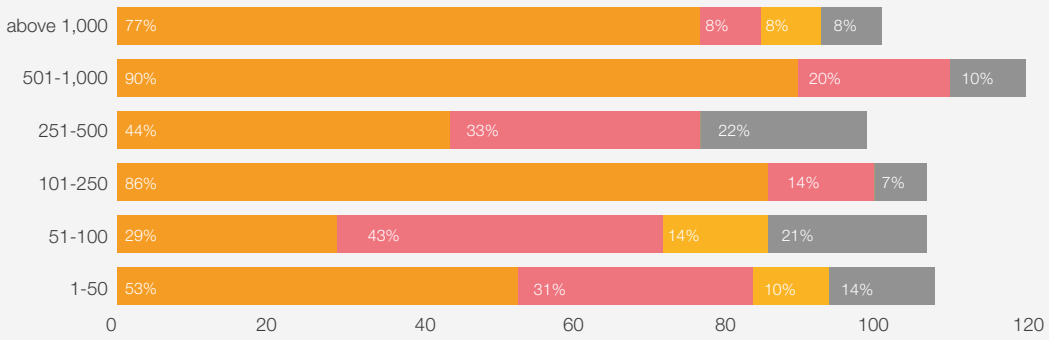
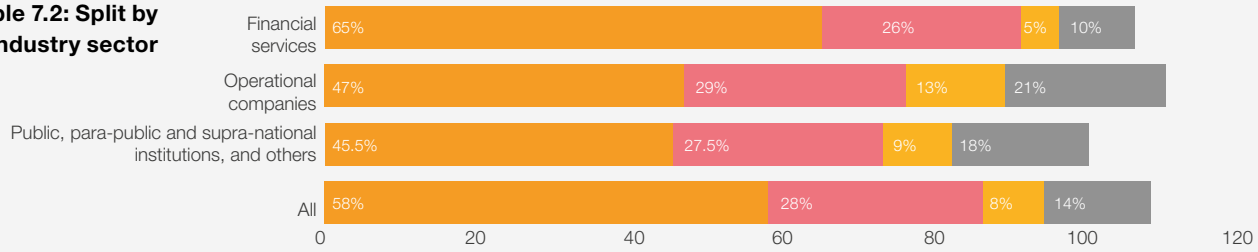


Table 7.2: Split by industry sector



- We have updated our contracts and we trust our critical business partners to be compliant
- We expect our critical business partners to obtain a third-party certification, to independently demonstrate their compliance
- We do not intend to take any specific action to ensure our critical business partners are compliant
- None of the above

8

Have you decided to appoint a DPO?

The Luxembourg Data Protection Authority, the Commission Nationale pour la Protection des Données ("CNPD"), should have seen roughly 50% of the respondents officially declaring the appointment of a Data Protection Officer ("DPO"). Of all the respondents, who have identified themselves as a public or para-public or supranational institution, only 55% responded that they have appointed and declared a DPO to the CNPD, an additional 18% have not yet taken a decision. A full 27% of such entities have analysed their situation and have decided not to nominate a DPO, which contradicts the definition given by the GDPR, which states being a public authority as one of the conditions obliging entities to nominate a DPO.
More generally, we still see a number of respondents not having analysed whether they need to appoint a DPO. This questions their compliance and their accountability framework.

Table 8.1: Split by company size (number of employees)

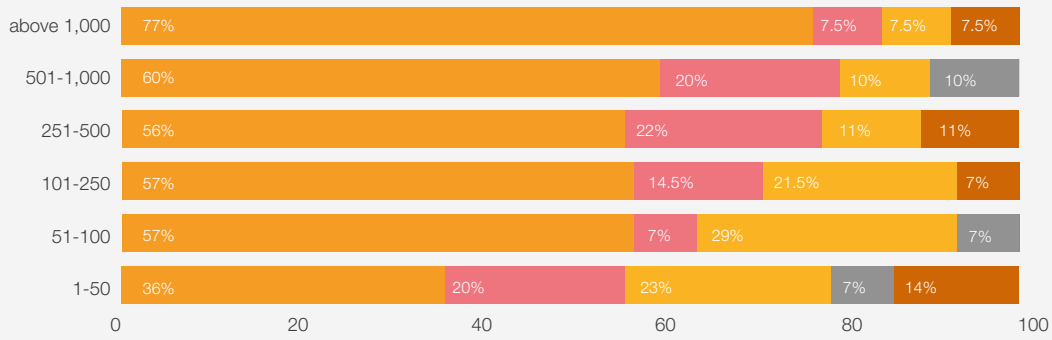
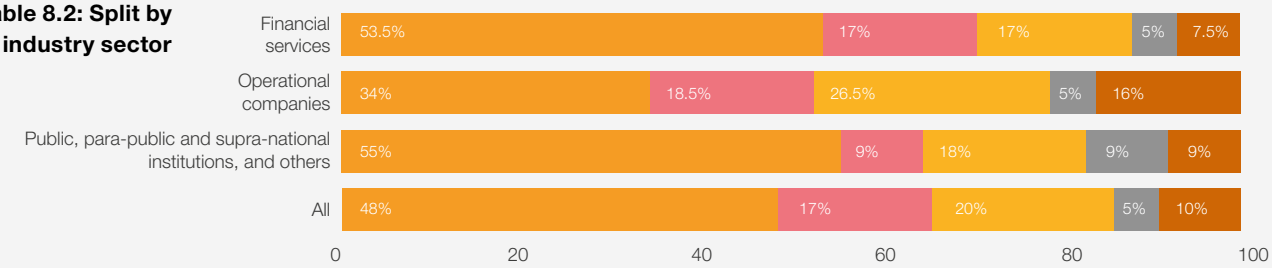


Table 8.2: Split by industry sector



- Yes, we have analysed our situation: we have decided to appoint a DPO and declared him/her to the CNPD
- Yes, we have analysed our situation: we have decided not to appoint a DPO and have formally documented this decision
- Yes, we have analysed our situation: we have decided not to appoint a DPO but have not formally documented this decision
- Yes, we have analysed our situation: we have not yet made a decision
- No, we have not made the analysis whether a DPO is necessary or not

9

Does your organisation have procedures regarding transparency and data subject rights?

Entities within the financial services have an edge over the other industries in terms of implementing transparency procedures, reaching nearly 90% in terms of responding to the transparency requirements of the GDPR. About 75% of operational and other non-financial entities have implemented such transparency procedures.
Even if these are relatively high numbers, responding to data subject requests still remains an ad hoc task in nearly a third of the cases.

Table 9.1: Split by company size (number of employees)

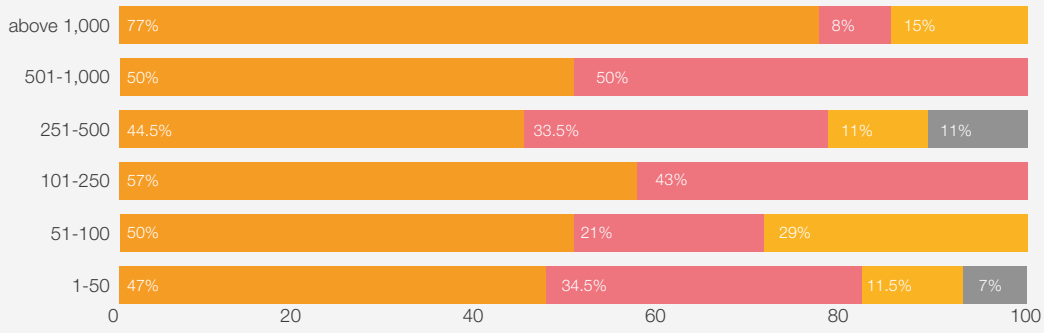
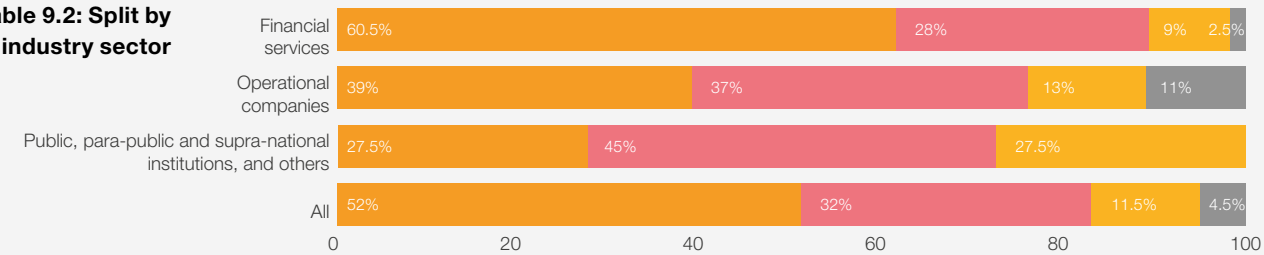


Table 9.2: Split by industry sector



- Yes, the procedures have been drafted and implemented, including updating our privacy notices
- Partially, privacy notices have been updated, data subjects can exercise their rights, but the response process is not systematically described in a document
- No, we have not yet updated our privacy notices; yet data subjects can exercise their rights via a standard contact form
- No, we do not plan to put these in place

10

Have you already received requests from data subjects to exercise their rights?

About a third of the entities have had to deal with a request of a data subject. In the majority of the cases, organisations had to deal with one to three requests. About 8% of the respondents have already dealt with more than seven requests and 5% have received between four and six data subject requests.
There is a clear link between the number of data subject requests received and the number of employees, where the largest entities have to deal with the largest amount of requests.

Table 10.1: Split by company size (number of employees)

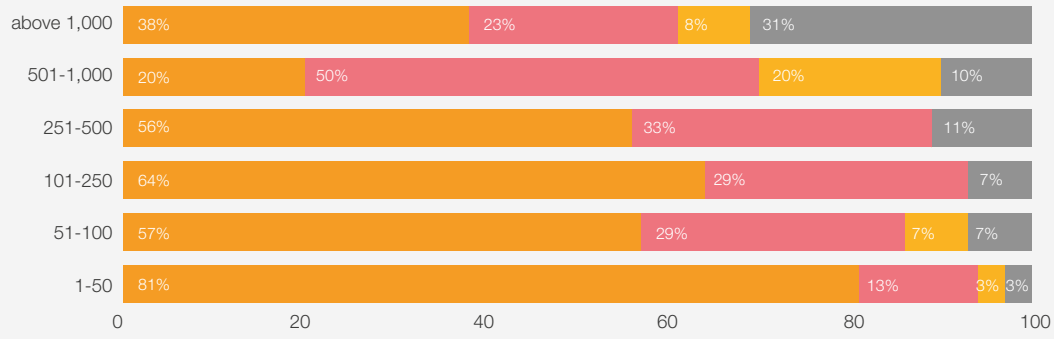
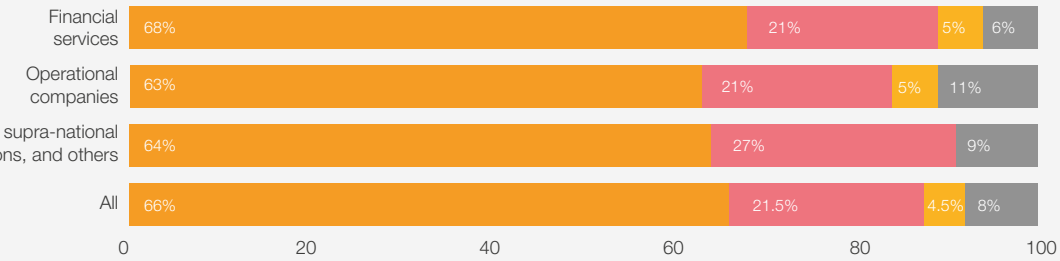
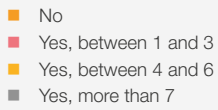


Table 10.2: Split by industry sector





11

Does your organisation have procedures regarding personal data breaches management?

In case of a data breach, nearly a third of the respondents would be dealing with this event "on-the-go", as they either have not implemented data breach management procedures, or have not identified the staff who will be dealing with these. The financial services actors seem to be quite ahead in terms of readiness to respond to personal data breaches, as close to 80% of such respondents have the necessary procedures in place, yet in certain cases, the teams are still to be fully trained.

Table 11.1: Split by company size (number of employees)

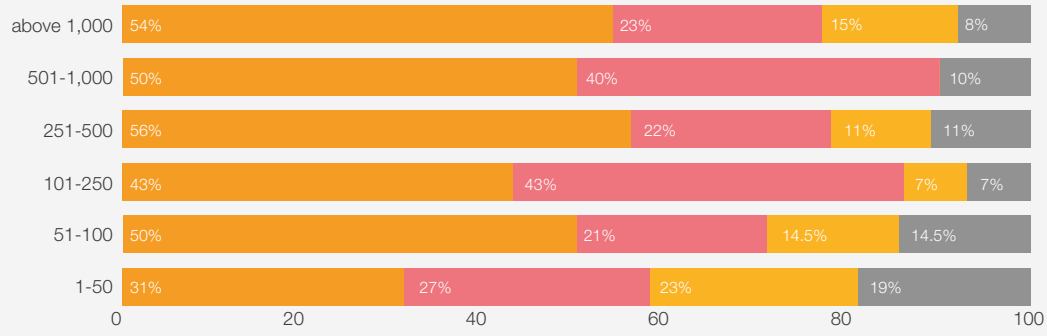
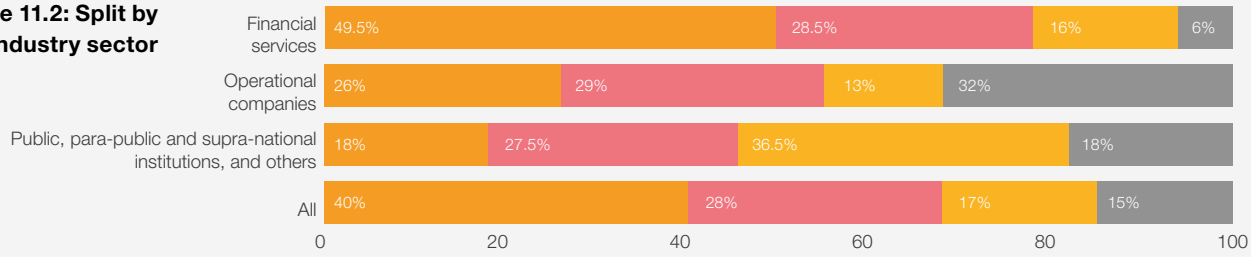


Table 11.2: Split by industry sector



- Yes, the procedures have been drafted and implemented, including the management of an internal data breaches record, notification to the supervisory authority and information to the data subjects when applicable.
- Partially, the procedures have been drafted but the teams are not yet totally informed and trained in regards of personal data breaches management
- Partially, the procedures are being drafted and implemented
- No, we have not yet implemented data breaches management procedures

12

Has your organisation already faced a personal data breach?

The former CEO of Cisco, John Chambers once said, "There are two types of companies: those that have been hacked, and those who don't know they have been hacked." Therefore, it comes as quite a surprise that a full two thirds of the respondents are confident that they have not been victims to a breach of personal data. Less than 30% of the entities admit having faced a personal data breach, whilst only 5% of the respondents probably share John Chambers' views and indicate that they do not know if they have faced a personal data breach or not. Generally, the larger the company, the more probable it is that a personal data breach would have already occurred. Note that the question addressed all personal data breaches and not just those reported to the CNPD.

Table 12.1: Split by company size (number of employees)

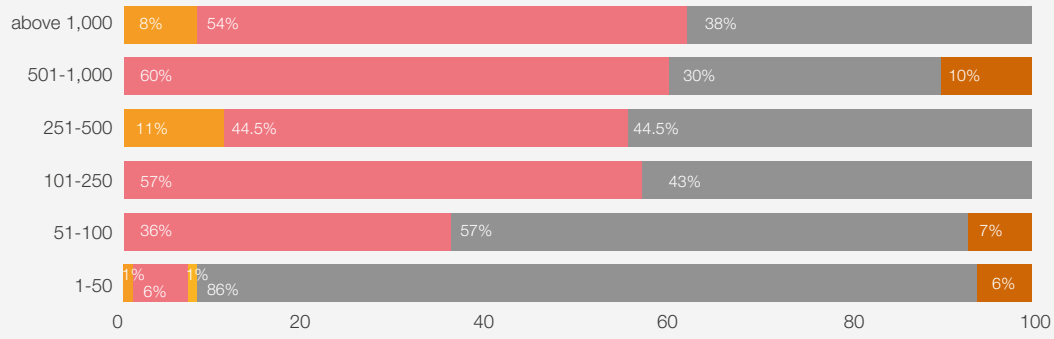
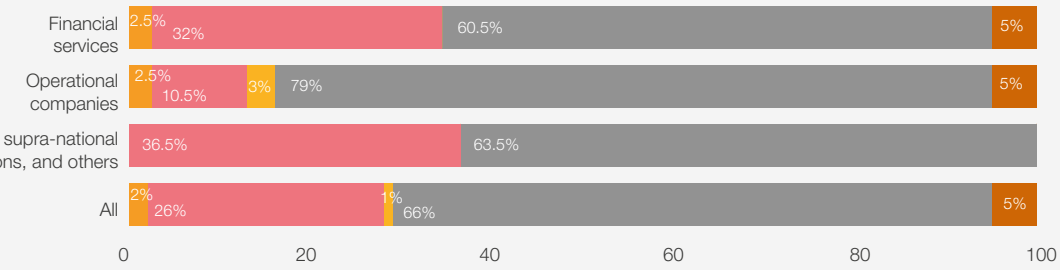


Table 12.2: Split by industry sector



- Yes, we have already faced a data breach that could have severe impacts for the concerned data subjects
- Yes, we have already faced a data breach that could only lead to no/minor impact for the concerned data subjects
- Yes, we have already faced a data breach but we don't know how to assess the potential impact of a data breach for the concerned data subjects
- No, we have not faced any personal data breach yet
- We don't know if we already have faced a personal data breach

13

Have you conducted a data security analysis of the data protection measures within your organisation?

One of the seven core principles of the GDPR states, "personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures." Nevertheless, more than 35% of the respondents have indicated that they have not yet conducted a data security analysis. An additional 26% indicate that the level of security measures will have to be increased or modified; yet this has not prevented 90% of the entities to feel compliant with the GDPR, admitting that additional measures are still to be taken in certain cases. Only one third of the entities have assessed their data security and feel these security measures are satisfactory.

Table 13.1: Split by company size (number of employees)

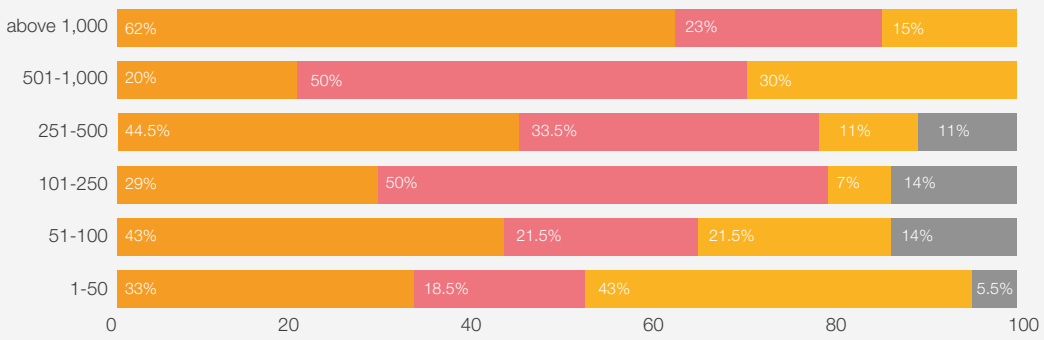
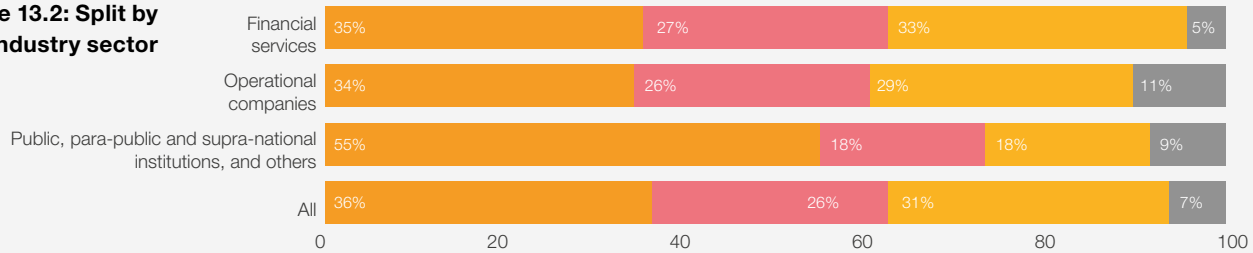


Table 13.2: Split by industry sector



- Yes and the level of security measures is satisfactory
- Yes, however the level of security measures will have to be increased/modified
- No, however this analysis is planned in the next months
- No, we do not plan to analyze the security measures within our organisation

14

Do you envisage financial investments in security measures following the implementation of the GDPR?

The majority of entities with more than 500 employees have either already invested into additional security measures, or are planning to do so. In general, around 40% of the organisations feel comfortable with the security measures in place and an additional 16% feel that additional financial resources would be necessary to improve the security measures, these resources being unfortunately not available right now.

Table 14.1: Split by company size (number of employees)

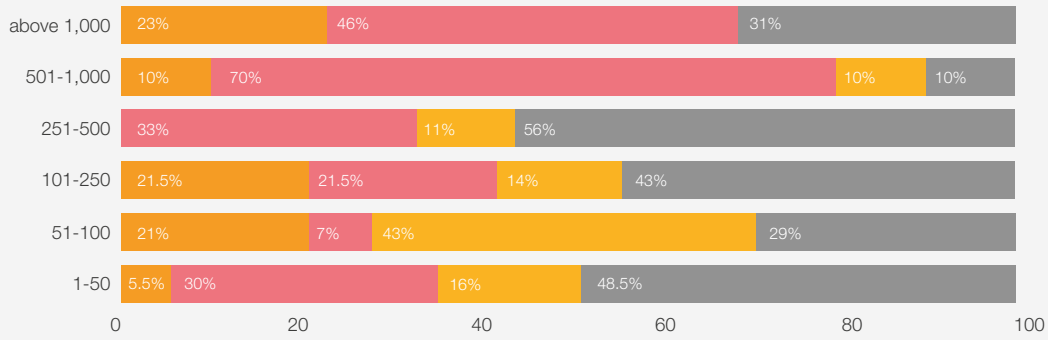
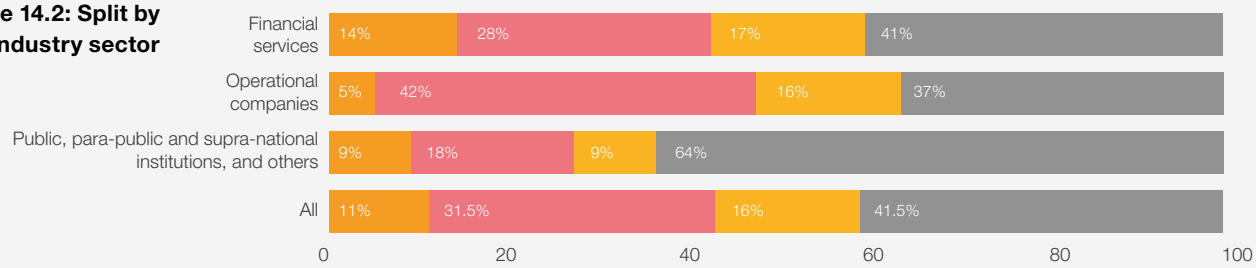


Table 14.2: Split by industry sector



- Yes, we have already an approved budget and we're using it
- Yes, we are thinking about it
- No, we do not have the necessary financial resources for such investments
- No, our security measures are sufficient

15

Would your organisation consider becoming CARPA-certified?

(CARPA stands for Certified Assurance Report Based Processing Activities, the GDPR certification mechanism developed by the CNPD)

Less than 5% of Luxembourg-based entities plan to pursue a GDPR certification. Half of the respondents have indicated that they do not intend to become CARPA certified and the remaining 45% claim they have not yet made up their minds. Time will tell whether the CARPA certification will be a sought for "assurance" by entities or whether a "mutual" trust in terms of GDPR compliance will remain common in the marketplace.

Table 15.1: Split by company size (number of employees)

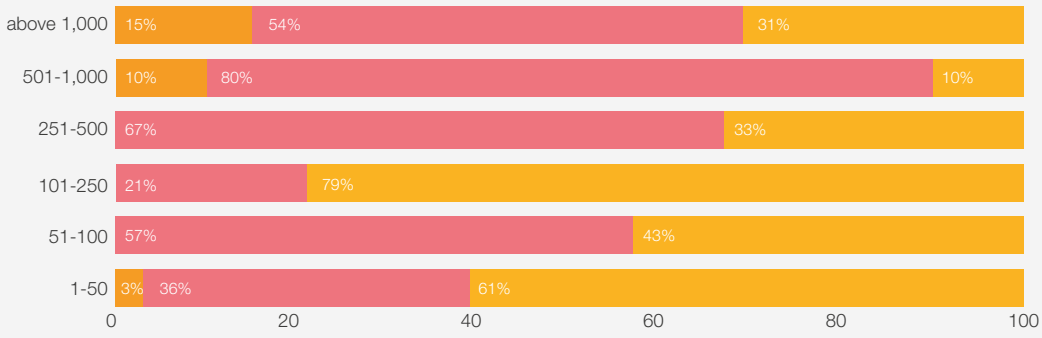
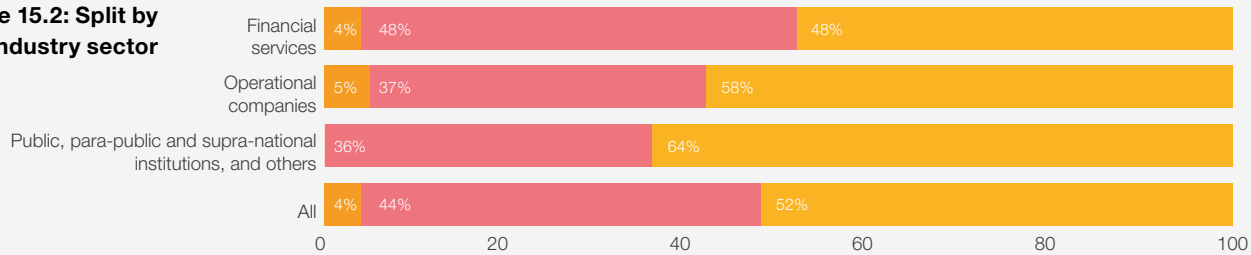
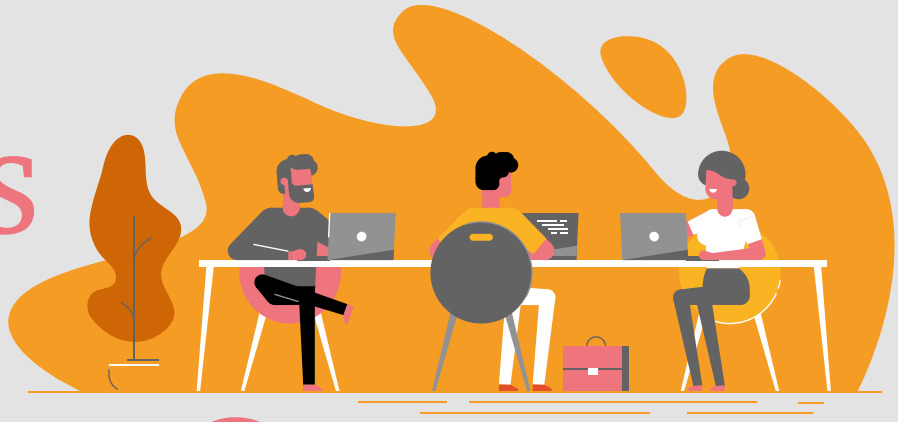


Table 15.2: Split by industry sector



- Yes, our company plans on obtaining the CARPA certification
- We have not yet made a decision on whether obtaining the CARPA certification
- No, we are not interested in obtaining the CARPA certification

Key findings



1

Around half of the respondents consider that they fulfill the majority of the requirements required by the GDPR. An additional 40% feel they are close to being ready to meet the Regulation imposed requirements. Among the respondents, the entities from the financial services are ahead in terms of maturity, 52% of them having implemented most of the requirements and changes of the GDPR.

2

Half of the respondents have identified the risks for data subjects, but have not mitigated them yet, which suggests that the core principle of the Regulation is not fully respected yet in 50% of the cases.

3

The mapping of all the personal data processed is the key challenge for the majority of the respondents.

4

Defining and documenting the retention periods for all the personal data processing remains a pain point throughout all industry sectors.

5

The majority of the respondents have not conducted a Data Protection Impact Assessment and 10% of them do not plan to do so, which raises questions how the risks are assessed and how appropriate safeguards are put in place.

6

Around half of the respondents recognised the need to update their internal audit plan with the data protection requirements and thus conduct a GDPR audit in 2019.

7

The majority of the respondents are confident their counterparts are GDPR compliant and have also updated the contractual/legal documentation.

8

The appointment of a Data Protection Officer is an important question raised by the GDPR, which triggered many thoughts for all the respondents. Half of the respondents declared the appointment of a DPO to the CNPD.

9

The vast majority of the respondents, whatever the industry, implemented the documentation in terms of procedures and the transparency of processing.

10

A third of the respondents have had to deal with a request of a data subject, with the number of requests increasing proportionally to the size of the entity.

11

Except for the majority of financial services sector entities, most of the remaining respondents are not fully ready to cope with a personal data breach, either in terms of documentation, or in terms of staff readiness.

12

Almost 70% of the respondents are confident they have not faced a personal data breach. This high figure raises questions, as potentially, entities could have faced a personal data breach without actually being aware of it.

13

Data security practices are not the main problematic of the respondents as only one third of them have analysed the current security practices and measures; yet in general, 90% of the respondents consider themselves as GDPR-ready or “ready in the near future”.

14

Only a small percentage of entities have already invested into new security measures and another 32% are thinking about doing so. Yet more than 40% consider their security measures as sufficient and thus are not willing to make additional resources available to enhance their security measures.

15

The CARPA certification is not an agenda item for around 90% of the respondents.

Contact

Frédéric Vonner
GDPR and Privacy Leader
+352 49 48 48 4173
frederic.vonner@lu.pwc.com

Thank you