



Privacy Survey 2021

Insights



Privacy Survey

This survey provides valuable insights into the challenges around data protection within organisations. 50 privacy professionals in the Netherlands participated in January and February 2021.

Key focus areas:

- Insight in the key themes around data protection and privacy management. This helps you to get a better feel for privacy developments relevant to your organisation and it gives you a unique insight into what other organisations are doing to ensure sustainable privacy management.
- Insight in the impact of working remotely during COVID-19 on privacy and security.

Survey respondents:



44% Privacy Officers



5% Compliance & Legal Counsels



21% Information & Security Managers/Officers



30% other (HR, Controller, etc.)

Size of organization (number of employees)

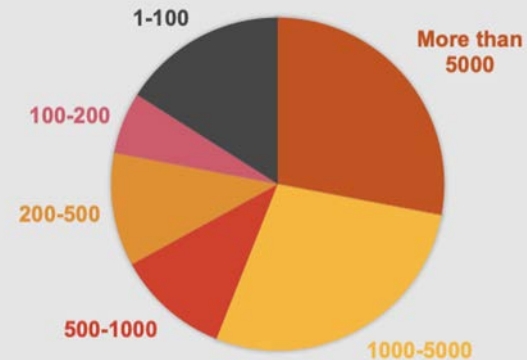


Table of Contents

Privacy & COVID-19 4

Privacy Maturity 5

The next steps 7



Privacy and COVID-19

91% of the employees is working from home since the lockdown. 83% of the organisations say working remotely has had an impact on the security of personal data and privacy. What was that impact?

40%

Is more aware of privacy and security risks since working from home.

58%

Invested in additional measures to ensure a secure work environment at home.

Data breaches did not increase

50% of the organisations say that the number of data breaches is comparable to last year (the year before the corona lockdown). In 21% of the companies the data breaches even decreased.

Only 8% of the increase in data breaches was related to working at home.

Overall the Privacy budget in 2021 was equal or increased compared to 2020. Only 6% of the organizations cut the privacy budgets.

36%

Say the budget increased.

Privacy Maturity in 2021

Last year, the biggest challenge in maintaining adequate privacy and data protection was creating privacy awareness. This year, organisations see keeping track of the various processing activities as the biggest challenge, together with the implementation of retention periods. The challenges are not completely in line with the top 3 key areas of focus for organisations.

Top 3 privacy challenges:



Data register (16%)



Data retention & Deletion (11%)



Awareness (10%)

Top 3 privacy focus:



Awareness (18%)



Privacy by Design (15%)



Tooling (14%)

AI

50% of the organisations is using Artificial Intelligence (AI) for user convenience, targeting and business processes. Users are however not always informed.

30%

Of participants say that they do not know how to prevent negative impacts on users, such as discrimination or exclusion by AI. Privacy assessment are not part of the process, or no privacy policy for AI is implemented.

Schrems II

Almost all organisations evaluated the impact of Schrems II on their data processing.

For more information on the impact of Schrems II:
<https://www.pwc.nl/nl/actueel-en-publicaties/themas/digitalisering/hof-van-justitie-europese-unie-zet-streep-door-privacy-shield.html>

57%

Did not take measures regarding Schrems II. 31% say that they will wait for the processor to solve the problem. 26% did not take any action.

Data Breaches

80% of the organisations did not notice an increase in data breaches compared to last year. Also the impact of the data breaches is not different.

60%

Of the increase in data breaches was a wrongly send file or email. People are still the biggest threat for data breaches.



The next steps

Privacy to a higher level

5 steps to build sustainable privacy in your organisation.

- 1** **Insights in data processing**
Set up your RoPa
- 2** **Privacy control framework**
Staying in control
- 3** **Data retention**
Make it concrete
- 4** **Privacy Technology**
Make your privacy life easier
- 5** **Privacy Certification**
Building consumer trust

Keeping insight in data is one of the top challenges for organisations. However, only 30% is using technology to support them in managing the data landscape.

16%

Says the keeping insight in data processing is one of the key challenges

Insights in data processing

As the data landscape constantly changes, via different means, technologies can help organisations to identify their data landscape and manage data in a structured and sustainable manner. This is achieved by addressing two main perspectives, identity and access management, and the data landscape itself.

The top 3 of technologies that we see at organisations regarding data management:

Data discovery

Systems that analyse both structured and unstructured data across an enterprise to identify personal data.

Data mapping

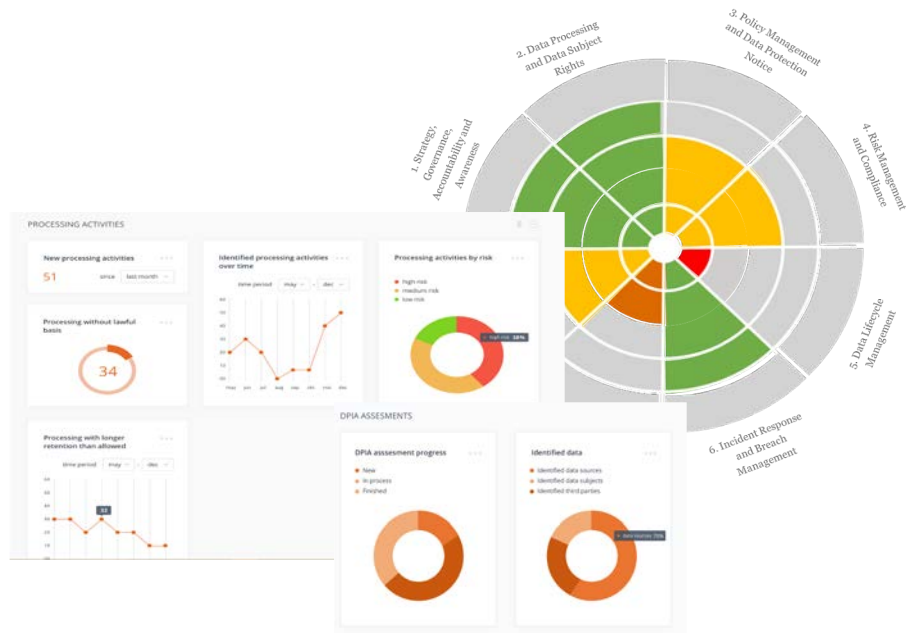
Systems that tag all data related to an individual and can demonstrate how all elements link together.

Consent management

Systems that manage, track, and demonstrate all relevant GDPR consent provisions.

Privacy control framework

66% of the organisations implemented a privacy control framework. 42% is using a privacy control framework that they developed themselves, 12% is using the NOREA framework where 12% is using other frameworks, from for example Nymity and ICO.



Only 15% of the organisations is using technology to monitor the privacy control framework. 55% is monitoring the PCF manually (e.g. via assessments or in-control statements).

Key drivers for implementing a PCF

- Sustainable compliance with data protection regulations
- It shows to clients, suppliers and other stakeholders that your organisation is a trusted digital partner.
- Transparency throughout the organisation
- Allows you to deduplicate controls and thus effort based on control objectives by aligning on other frameworks in your organisation (e.g. security, risk).

Organisations are faced with challenges when implementing their retention schedules. Legacy applications do not have proper deletion functionality and system interconnectedness lead to corrupt references. On top organisations have data related to the same data subject scattered in both unstructured and structured repositories. Tackling this challenge requires an understanding of how processes and systems interrelate in order to apply the right deletion strategy.

Data Retention

70%

Does not use technology to assist in identifying, classifying and managing the data landscape (e.g. retention and deletion). While this is one of the biggest challenges for organisations.

35%

Of the organisations want to use technology in the future.

Key drivers for data retention & deletion:

- Compliance with the GDPR requirement to keep data no longer than necessary for the purpose for which it was collected & executing data subject requests
- Reduce risk exposure - recent data breaches often contained data which should have been removed
- As part of data protection by default and design effort to ensure new tools address retention when they are procured or built

Privacy Technology

The GDPR, among other things, requires organisations to manage their privacy framework in a sustainable and manageable manner and defines specific aspects for it, including accountability, Records of Processing Activities, data protection by design, DPIA and breach notifications. Technology can play a significant role in helping the organisation to maintain its privacy program and framework, over the various aspects in a sustainable way.

Top 3 privacy challenges:



To assist in privacy management (85%)



To assist in identifying, classifying and managing the data landscape (30%)




To monitor the privacy control framework (15%)

Key challenges

- Limited overview of data processing e.g. due to many shadow systems
- Inefficient consent management and lack of data control by your customers
- Inefficient processes that are reliant on manual labour for privacy compliance
- Technology that fails to support a structured way of reporting.

Key drivers

- Being continuously in control
- Managing incidents effectively
- Reducing compliance costs
- Increasing competitive advantage by creating a single view of your customer
- Automating consent management while improving the customer experience



Markets and customers are increasingly expecting and demanding trust and transparency with regards to privacy

Privacy certification

39%

of the organisations is able to prove privacy compliance via a report or certification. 23% via an assurance/audit report.

30%

of the organisations is interested in privacy certification.

Key drivers for external trust and transparency:

- New and strengthened Privacy & Data Protection laws rising around the world
- Regulatory developments (e.g. Schrems II)
- Consumers are becoming increasingly privacy sensitive
- Customers demand trust and responsible data processing



Thank

You



Bram van Tiel

Partner

T: 31 (0)88 792 53 88

E: bram.van.tiel@pwc.com



Yvette van Gernerden

Partner

T: +31(0)652 00 59 24

E: yvette.van.gernerden@pwc.com



Sandra Mochèl

Director

T: +31 (0)6 533 53 641

E: sandra.mochel@pwc.com



© 2021 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.