Whitepaper Special

Creating support and urgency for GDPR privacy compliance programs

In collaboration with Annemarie Vervoordeldonk | Privacy Consultant

privacy perfect

Make sure.

INTRODUCTION

Until a year ago, many people had not even heard about the GDPR. Trying to get a company into preparing for this new legislation used to be quite hard, simply because there was no sense of urgency outside the ‘inner circle’ of data protection officers, who seem to be the only ones with knowledge about what was coming. Now that the GDPR has been in force for a while, the urgency for an effective privacy compliance program has only increased.

> *“This whitepaper is based on our extensive interview with Annemarie Vervoordeldonk, an experienced privacy professional.”*

This whitepaper sheds light on the circumstances under which such a program can succeed.
It is based on our extensive interview with Annemarie Vervoordeldonk, who worked for several multinationals in the role of privacy officer. Annemarie has now started her own business, providing consultancy and ‘DPO-as-a-Service’.

We have talked with her about the requirements for a successful GDPR privacy compliance program and our main findings are summarized here as **15 pieces of advice, grouped into three phases: A - preparation, B - execution and C - communication.**

A

First phase
Preparation

1

First things first: start with a privacy governance framework

Start with formulating a privacy governance framework: which departments, roles and persons are responsible? What will be the organisation wide policies? Only after that is in place, is it possible to arrange the processes associated to this, such as getting a processing activity register in place, carrying out data protection impact assessments and registering (and notifying) personal data breaches. For this second phase, it is necessary to know which processes, applications and systems are being used within the organisation (see our whitepaper on this inventory here). This may sound obvious, but you cannot get the processes in order without having a clear organisation wide goal and structure for privacy governance.

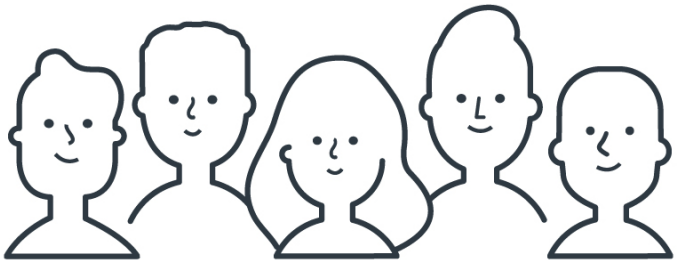
“Which departments, roles and persons are responsible?”

2

Tone at the top: effective privacy governance starts with backing from the board

Everything starts at the top of the organisation. Without backing of at least one sponsor of the program in the organisation's boardroom, a successful privacy compliance program is almost impossible. It's very hard to say how to get that sponsor, but anything or anyone helping you to be in touch with a potential sponsor will be useful. You may find a natural ally in the people responsible for HR, risk mitigation or compliance, but they should be in rather than just below the board. The Board is ultimately accountable for these activities and therefore has an interest in making the organisation compliant.

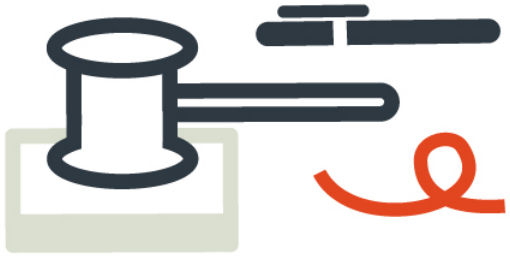
"Anything or anyone helping you to be in touch with a potential sponsor is useful."



3

Be multi-disciplinary: acquire necessary knowledge and involve other people

Although the GDPR is a legal instrument, you'll need at least some IT knowledge to be able to ask necessary questions. What if 'anonymisation' is in fact 'pseudonymisation'? You'd better find out early by asking the IT people you work with. A lack of 'ownership' threatens any GDPR privacy compliance program. Therefore, you need to involve other people with other responsibilities. Information security and privacy are basically two sides of the same coin - you'd rather team up to be stronger together.



4

Don’t mix responsibilities: you cannot combine executive and controlling roles

As a (chief) privacy officer (or data protection officer in GDPR speak), you need to be highly independent. You cannot combine that role with that of e.g. an HR director or an IT manager. Otherwise you would be assessing your own work and that is in contrast with the responsibilities that come with the role. The European Data Protection Board (EDPB) and the GDPR list requirements for this independency, such as responsibility for your own budget, reporting directly to the board, and access to support (staff and other resources).

5

Get your team together: you cannot do it alone

You’ve just been appointed as a privacy officer in a large organisation - and the board thinks that ‘that’s it’. Think again, board, we’re just getting started. To get the job done, a (chief) privacy officer needs a team doing the work, such as rolling out the privacy governance strategy and getting all procedures in place. What’s more, the procedures have to be followed, and that involves a lot of other people from the business, who have to be managed as well. A single person cannot do that on their own. So yes, you will need budget for that, and the organisation needs to provide for it.

“To get the job done, a (chief) privacy officer needs a team doing the work.”

B

• • •

Second phase

Execution

6

Get the programme managed: that too, is a job on its own

A good privacy officer is not necessarily a good program manager. So when getting your team together, consider hiring someone for the latter role, especially in large, complex organisations. You can focus on the subject matter and leave the organisation of the work to someone else. That can be a great relief to you and it can improve the effectiveness of the overall program by giving content and process equal weight. Remember that you need not and cannot be a specialist in all fields that are connected to, and relevant for privacy governance.

“Consider hiring someone as a program manager, especially in large, complex organisations.”

7

Build on existing foundations: there's stuff that you can reuse

The privacy governance framework may not be there, but other procedures will be. If the foundation is already there, why build a new one? Try to identify the most 'aligned' existing procedures and policies and build on them. That supports recognition, facilitates efficiency and increases return on investment. In many cases, there will already be extensive security policies, and these can be extended to match the needs for a GDPR privacy compliance program.

8

Be a people person: you need allies, lots of them

Privacy governance and privacy awareness are ninety percent communication. You need to team up with a lot of people in order to have eyes and ears across the whole organisation. This will pay back in terms of reduction of liabilities, created by the tunnel vision of individual departments. Informal communication lines are a must-have to get the information you need. People have to be able to find you in order for you to build your inventories and ask you if an envisaged processing activity can be carried out.

> *"Try to identify the most 'aligned' existing procedures and policies and build on them. That supports recognition, facilitates the work and increases return of investment."*

9

What a surprise: all of a sudden, there are data breaches

Miraculously, after training the HR department, you get notified of (potential) breaches. Yes, breaches happened before, but they were not identified as such, so they never reached your desk. Training people means raising awareness, which will pay out - because an unnotified breach is a bigger liability than one that ends up on your desk. But note that this increase in breaches could be used against you at first. Prepare the Board to information that has been uncovered up till now. Understand that this is a sign of strength and not of weakness.

10

Switching initiative: people will follow your example

Once there is sufficient knowledge about the GDPR in your organisation, people will start contacting you spontaneously. Instead of having to be the ‘no saying’ privacy officer, you can switch roles. Questions will be formulated more carefully because people start realising that a project may have severe privacy implications. They will suggest themselves that maybe it’s not such a good idea after all. In such an atmosphere, you can be the ‘enabling’ party, helping to create the circumstances under which the project is possible after all.

C

Third phase

Communication

11

Diversify your communication: not everyone needs to know everything

Once you have decided that a breach of address data of five employees need not be notified to the supervisory authority because of a variety of reasons, make sure that you are selective in reporting the underlying reasons to the department involved. They might turn your context sensitive legal argument into a rule and bypass you on the next occasion. Transparency is good, but opacity sometimes better.

“Remember that most of the people you’re talking to are not familiar with legal nuance.”

12

Build a story about personal data: it's obvious to you, not to the rest

Yes, personal data is... personal data! But the people in your organisation will probably misunderstand the concept. Invest in a good story about what personal data is - people will be astonished if they realise that - yes, they are also processing that stuff that the GDPR is made of. Avoid ever-lasting discussions on whether IP addresses or data stored without a name but with a personal number is personal data. A good story explaining why most of the data processed is personal, will improve awareness and save you a lot of time.

"Making privacy your audience's 'own' property will help realise the importance of the subject"

"Invest in a good story about what personal data is."

13

Life is a box of chocolates: bring them at your training sessions

Life is a box of chocolates, but it shouldn't be full of surprises in the GDPR area. Making privacy your audience's 'own' property will help realise the importance of the subject. Ask the audience to stand up and start asking questions in the well known field of 'you have nothing to hide, right?'. Anyone not wanting to cross a border should sit down. Promise the last person standing a box of chocolate. If you have the right questions, you can keep the box for the next workshop or eat it yourself. Another way of relating to everyone's daily life is coming up with a few examples of recent data breaches and their consequences.

14

A data driven organisation: your organisation can be one too

Scepticism about the GDPR often prevails. The idea that you can actually benefit from becoming GDPR compliant is not yet widely recognised. Personal data will probably be very important to your organisation and its reputation, so knowing what is going on with them is important. Moreover, you can help spread the word. Shouldn't your organisation put personal data to work in a responsible manner? Even a company processing mainly HR data would benefit from doing so in a responsible and effective manner, so as to improve the loyalty and effectiveness of its workforce.

15

Fear, uncertainty and doubt: use them if really necessary

Yes, fines work. Competition law became a recognised threat in general compliance after huge fines on Microsoft were imposed by the European Commission. So the 4% worldwide turnover fines of the GDPR are a last resort in terms of bullying your organisation into proper privacy governance. Use with caution, but don't be afraid if you need to. Remember that the GDPR fines are a real liability and can be a pervasive argument for revenue and profit focused organisations to turn their attention to GDPR compliance.

PROFILE

ANNEMARIE VERVOORDELDONK

Annemarie is married and has two grown-up sons. Educated as a technical and scientific translator, she switched careers to become a legal counsel since 2006. Soon after, she acquired a specialisation in data protection law, and privacy became the core of her practice. She has previously worked as a privacy officer for two Dutch multinational companies; one family-owned, and the other listed. Currently, she is a privacy consultant at Quodata Privacy Services.

ABOUT PRIVACYPERFECT

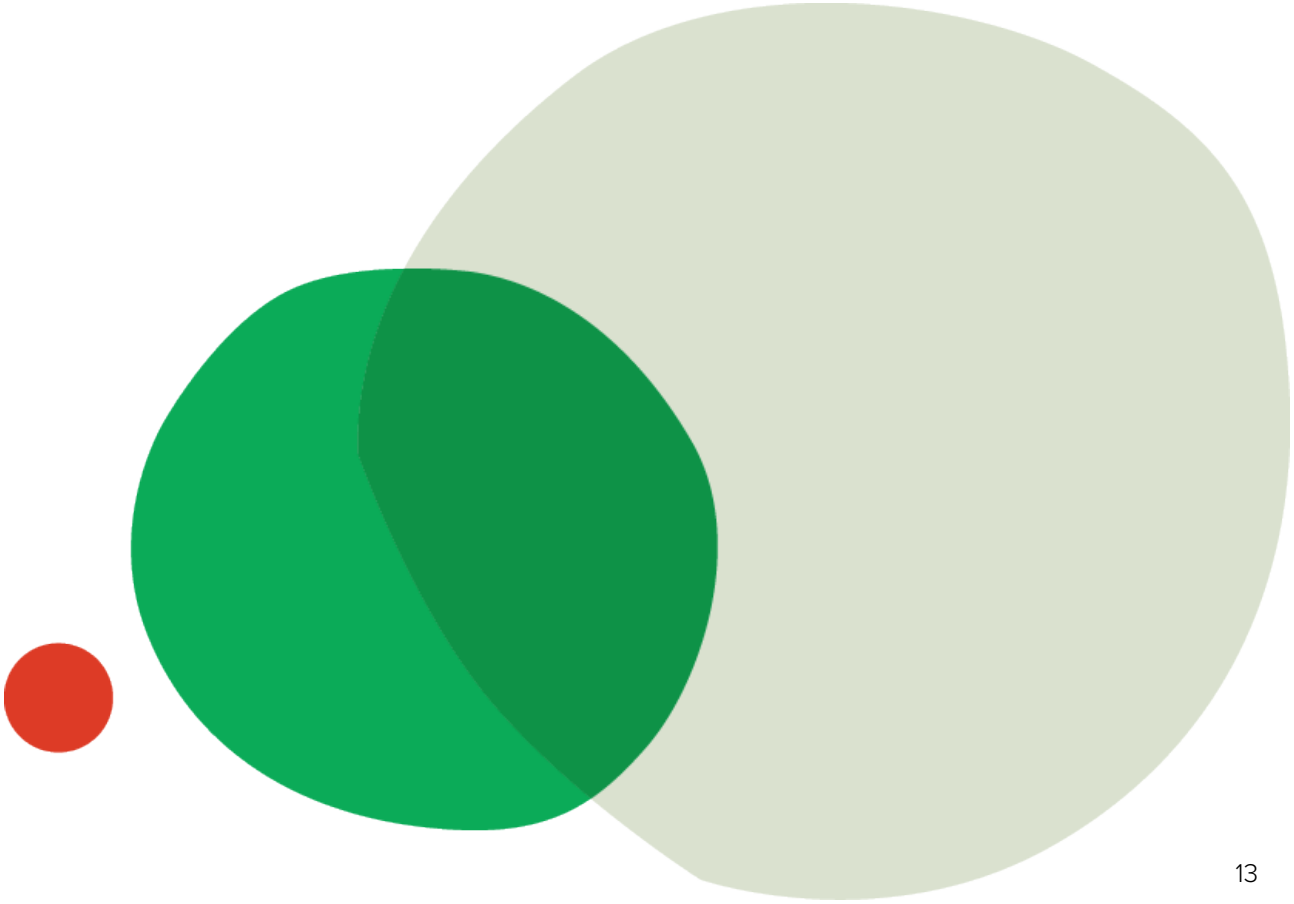
PrivacyPerfect is an easy-to-use GDPR compliance toolkit. It provides a natural flow between the three administrations required by the new regulation: data protection impact assessments, processing activities (including transfers), and data breaches. The user-friendly tool allows for maintaining all necessary privacy records and leading them through workflows to meet the needs of both SMEs and large companies.

MORE INFO

Do you have any questions regarding this whitepaper or would you like to get more information about the PrivacyPerfect tool? Please visit www.privacyperfect.com or contact us via info@privacyperfect.com.

CONTACT US

privacyperfect.com
info@privacyperfect.com
+31 10 310 07 40



Transparency

Compliance

Accountability

Connect with us

Linkedin.com/company/privacyperfect/

Twitter.com/PrivacyPerfect