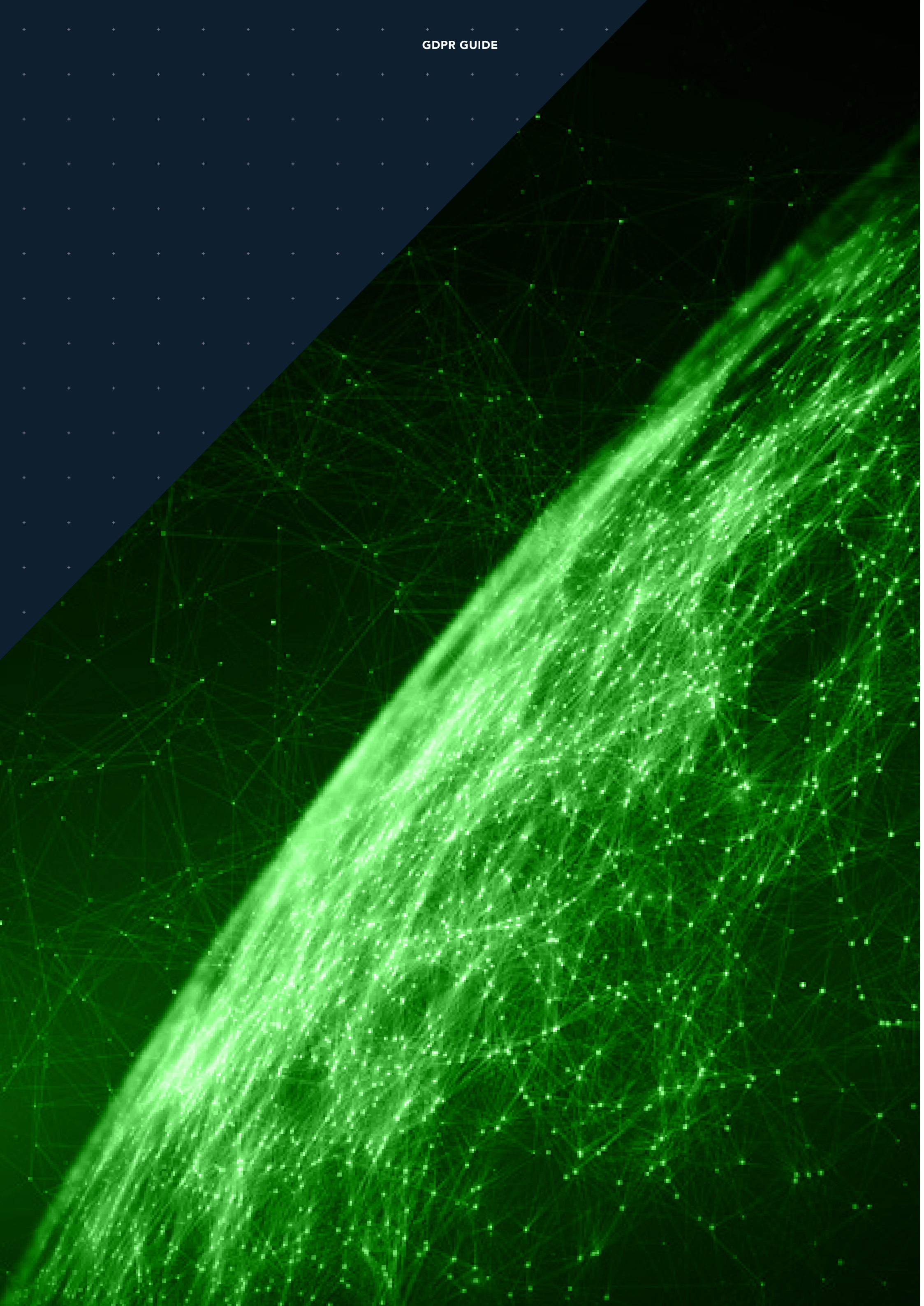
GDPR GUIDE

WHAT YOUR ORGANISATION NEEDS TO KNOW

By Eric Boonstra
CEO, EvoSwitch

evoswitch



GDPR GUIDE

what your organisation needs to know

The General Data Protection Regulation [GDPR] – the EU's new regulation covering protection of personal data - becomes law in May next year. The new legislation tackles inconsistencies in the current data security landscape and tries to ensure the secure free flow of data between member states while protecting the personal data of EU citizens.

Not everyone is ready. According to Gartner, more than 50 percent of companies affected by the GDPR will not be in full compliance with its requirements by the deadline.

This could be costly. Failure to meet the GDPR's standards could lead to fines of up to €20 million or 4% of your global annual turnover. If you do not have a full plan yet you need to make one and start implementing it soon.

There is a lot of information circulating about what you need to do, which is useful but also potentially confusing. So we have prepared this step-by-step overview of the process addressing the key things you should consider and actions you could take.

As experts in the physical hosting of the affected data, we believe that data center operators should take a proactive role, offering support and advice wherever possible. So, in addition to providing this planning paper we offer GDPR-specific consultancy for companies to support their ongoing assessment, planning and implementation efforts on the data floor.

Eric Boonstra
CEO, EvoSwitch

INDEX

GDPR GUIDE
what your organisation needs to know

COUNTDOWN TO GDPR

The GDPR takes over from the EU's Data Protection Directive of 1995, officially entitled 'Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data'.

2009 | Working Party on Police and Justice works with the European Commission [EC] to release a paper called the "Future of Privacy".

2010 | The EC creates a policy to protect individual data at the same time as reducing red tape and guaranteeing the free circulation of data in the EU.

2011 | The Committee for Civil Liberties, Justice and Home Affairs [LIBE] adopts a proposal on 'A comprehensive approach to personal data protection in the EU'; the EC Director of Fundamental Rights and Citizenship announces plans to harmonize data protection.

2012 | The EC proposes the GDPR as well as a Directive on Data Processing for Law Enforcement Purposes. The Data Protection Working Party publishes input on the data protection reform which welcomes the potential to significantly strengthen data protection in Europe.

2014 | The EU Justice Commissioner and Vice-President highlights the need for a uniform and modern data protection law for the EU that would build trust and generate growth.

2014 | The European Parliament votes in favour of GDPR, (621 in favour, 10 against and 22 abstentions). Reform≈now irreversible.

2015 | Common versions of the GDPR and the Directive of Data Transfers for Policing and Judicial Purposes agreed towards the end of the year. In December, LIBE adopts the result of the GDPR negotiations.

2016 | The 47 countries of the Council of Europe celebrate the 10th annual European Data Protection Day; the≈anniversary of the Council of Europe's Convention 108. The anniversary events include a conference on EU data protection reform.

2018 | The GDPR becomes law on 25 May.

"GDPR WILL HAVE A VERY BROAD TERRITORIAL SCOPE"

SCOPE: DO THEY MEAN ME?

Location: GDPR will have a very broad territorial scope as it is designed to affect any and every company that targets EU citizens. This means that it affects any company in the world that controls or processes EU data, regardless of whether the company is located in the EU or not.

GDPR applies to your organization if you:

- Employ any EU citizens
- Sell goods or services to people in the EU
- Run a website that uses technologies like cookies to monitor people in the EU
- Collect any sort of data that may include information about EU citizens

Size: While size makes a difference to the details, all companies need to comply with the new regulation.

Sector: GDPR covers a very broad range of data. With its focus on personal identifiable information, the regulation moves beyond commonly held data such as names and email addresses to include other identifiers such as phone International Mobile Equipment Identity [IMEI] numbers. For example, retail companies collecting data via eCommerce and loyalty cards must comply just as much as fitness applications that require users to submit dietary or exercise habits, if these are combined with personal registration details. The same principles apply to companies from all other sectors.

WHAT'S NEW?
KEY FEATURES

Greater Data Liability: Organizations will be more liable for the personal data they control and process.

Clearer Supervision: Data controllers must process all personal data in compliance with the GDPR and be able to show their supervisory authority: Each member state will have a single national data protection authority as the lead regulator for all EU compliance issues. In the Netherlands, for instance, this is the Autoritiet Persoonsgegevens based in Den Haag.

Active Consent: In contrast to the existing Data Protection Directive [DPD], the GDPR states that the individual will now need to actively give consent for their personal data to be processed, where previously implied consent was acceptable.

Accessible Records: Data controllers must provide an accessible and detailed record of how data is used, where and by whom.

Right to be Forgotten: Individuals will have a statutory "right to be forgotten" if a data controller can no longer provide a legitimate reason for keeping their data.

Right to Portability: They will also have a right to move their data, meaning they can request data from an old controller in a readable format, and move it from one provider to another.

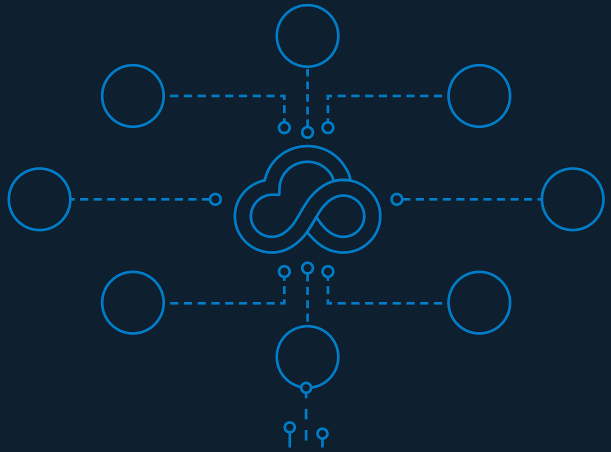
New Processor Responsibilities: Data processors (as opposed to data controllers, who collect the data and are ultimately responsible for it) will be regulated under the GDPR for the first time. Going forward they will need to work closely with data controllers and:

1. Maintain detailed records of processing operations and activities
2. Implement appropriate security standards
3. Carry out routine data Protection Impact Assessments [PIAs] for high risk projects
4. Appoint a Data Protection Officer
5. Comply with rules on international data transfers and co-operate with national supervisory authorities

GDPR ROADMAP

1 Internal Engagement

GDPR is not an “IT only” challenge. It goes to the heart of a company’s business model, and should have a direct impact on employee rights, behaviour and customer engagement. The fines are also significant enough to create a major business risk, whatever the size of your business. So do not go after it alone. Discuss the regulation, its implications for the business, and the opportunities and challenges it presents at board level. You will need their understanding, commitment and support. Consider creating a multi-disciplinary team to drive the changes, covering everything from HR and Legal to Procurement and Marketing.



COVERING YOUR SAAS

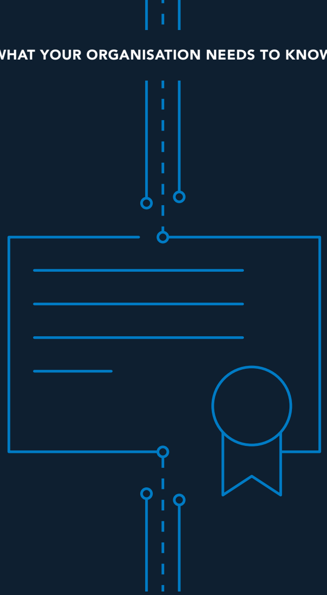
Shifting business processes to SaaS offers huge benefits and enhances business agility. But according to some studies there is a huge discrepancy between thenumber of ‘official’ SaaS platforms and ‘unofficial’ or ‘shadow’ services, all of which will need to be covered for GDPR. A 2016 study by Symantec claims that “the average enterprise organization was using 928 caloud apps, up from 841 earlier this year. However, most CIOs think their organization only uses around 30 or 40 cloud apps.”

GDPR ROADMAP

2 Audit

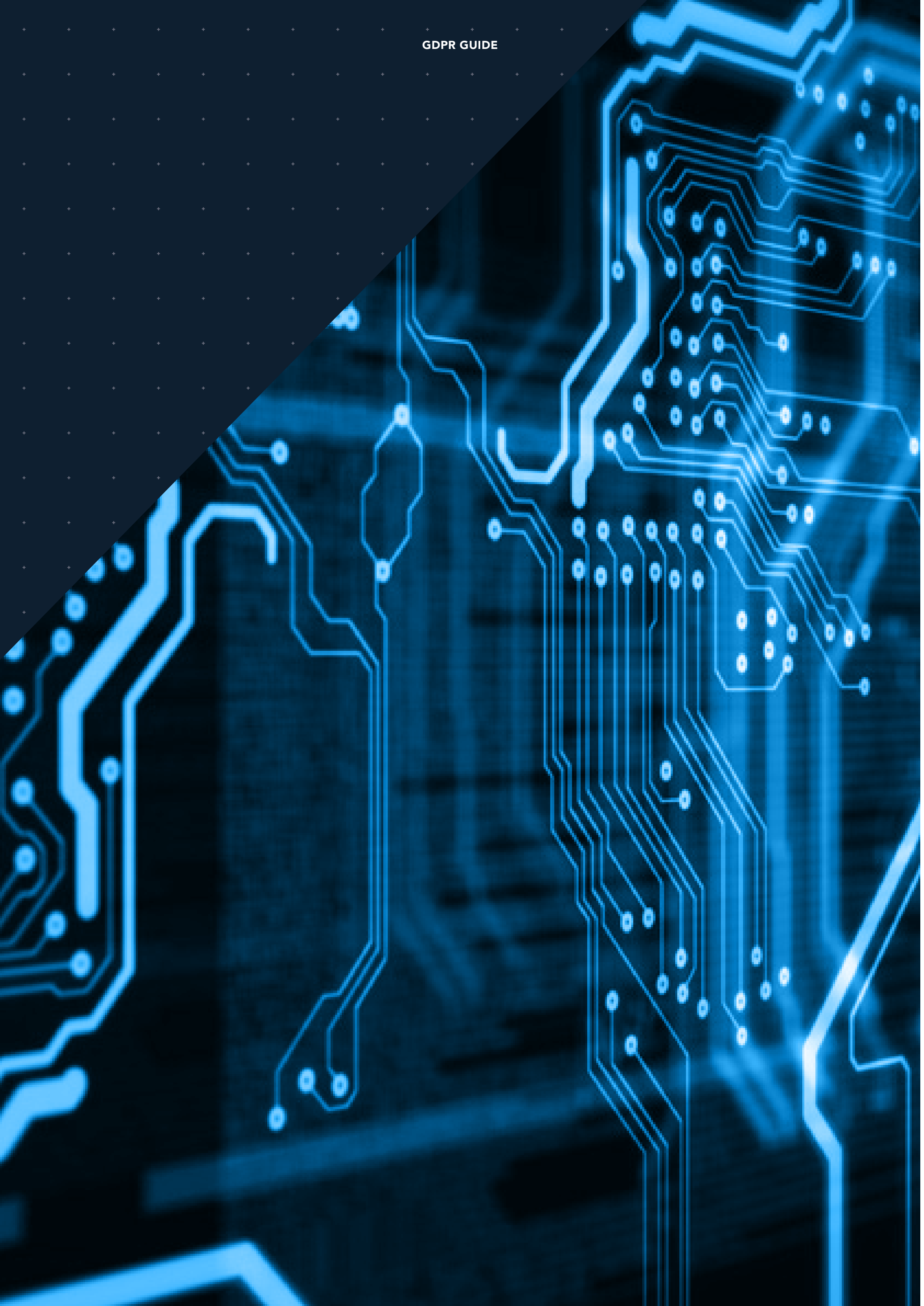
First read the regulation; there is a link at the end of this paper and it is surprisingly well expressed. Then assess your current situation so that you know how much you need to change and where. Doing this will help you to comply with the GDPR's accountability principle:

- **Data Audit:** Makes sure you know where all your data lives and who has access to it. As well as a pan-organizational review, this may require separate audits in particular business areas.
- **Partner Audit:** Make sure every service provider or partner that has access to your data is also compliant with GDPR, and operates under an officially sanctioned data jurisdiction.
- **Device Audit:** List every single device that has access to personal data.
- **Privacy Notices Audit:** Review your current privacy notices and where they will need to change to conform with the GDPR – e.g. in making them easy to understand, in explaining your lawful basis for processing their data, your data retention periods and where they can complain.
- **Consent Audit:** Review how you seek, record and manage consent and whether you need to make any changes.



COMPLIANCE TRACKER

Put together a track record of compliance for the 6 months or 3 months (whatever is manageable) leading up to next year's deadline. This will help you test the new process and at the same time as demonstrating to your national data authority that you are taking the transition seriously.



GDPR ROADMAP

3 Design

Bearing the results of the above audits in mind, new and revised policies, processes, and an implementation plan need to be designed, agreed and resourced.

Individual rights are central to the GDPR, and should be your key considerations in process design. The GDPR is built around the following rights for individuals:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure (aka 'Right to be forgotten')
- Right to restrict processing
- Right to data portability
- Right to object
- Right not to be subject to automated decision-making, including profiling.

However, many of these rights are already supported by current law, so transition should be relatively easy. The new right is data portability. If someone wants their data moved can you locate and delete the data? Who will make the decisions about deletion? What format will the data be provided in? Can you easily contact and effect removal of copies via any partners with whom you have shared that data?

DIY Data Management: If your organisation handles a large number of access requests, consider the implications of having to deal with more data requests at no cost and in a shorter timeframe. Is it feasible to set up a system that allows individuals to access and edit their information easily online?

Active Consent: Your process design should also pay close attention to your data consent mechanisms, which must include active consent, must be unbundled from other T&Cs, and cannot include pre-ticked consent boxes. Parent or Guardian Consent may well be required if you offer 'information society services' to people younger than 16. Consent should also be granular (offering options), thoroughly documented and easily withdrawn.

'Privacy by design and privacy by default' become express legal requirements under GDPR. This means that all data processing design must be seen to implement data-protection principles, as well as ensuring that only the personal data 'necessary for each specific purpose' is processed. For example, an app should not register the users' location if that is not necessary. Or if someone wants to subscribe to your newsletter, you may not ask for more information than is necessary.

MITIGATING IMPACT: PIAS

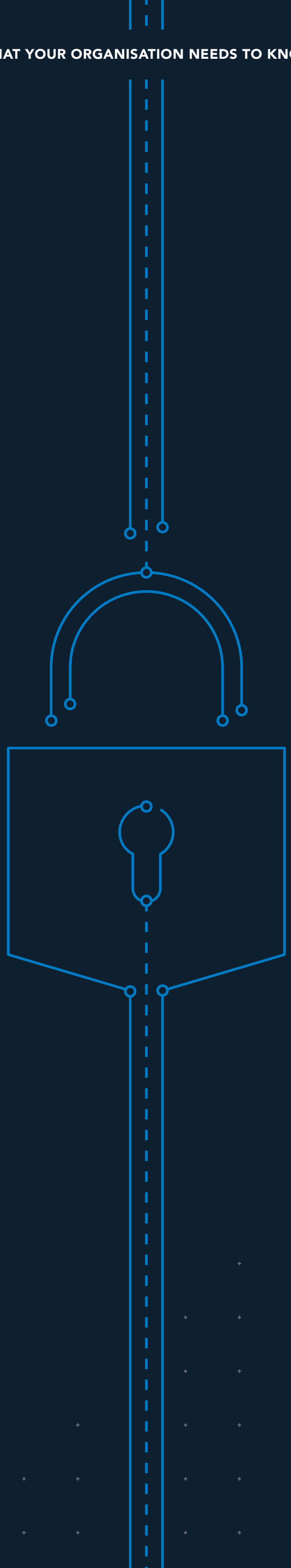
If the data you process could lead to a high level of privacy risk you may have to make a Protection Impact Assessment [PIA], mapping out this risk and setting out measures to reduce it. Your data authority may need to review and give a legal opinion on this.

GDPR ROADMAP

4 Access Definition

Access definition is the key to company data security, helping to keep track of who has access, and to prevent a single breach granting access to everything. If you do not already have systems in place you should:

- **Establish administrative privileges:** Make sure administrative actions can only be taken by a select few, to minimise the risk of others gaining control of the network.
- **Build tiered access to personal data:** Control access to data on a need to know basis. This should be based on the user, device and the network from which the request has come.
- **Set remote access rights for company data:** Make sure you can retrieve and erase data from all devices with access to personal data, especially in the event of loss or theft.



GDPR ROADMAP

5 Capacity Building

Do you need a *Data Protection Officer* [DPO]? The answer is 'probably' – and if not, you should add the responsibilities of DPO to an existing role. You are obliged to appoint a DPO if you are a public authority, if you conduct mass monitoring or large-scale processing of specialist data. But even if these do not apply, the role is an important one with significant responsibilities.

Training: Do not underestimate the importance of training for data security. There is no point in investing in cutting-edge scan and security software if employees are not educated in basic cybersecurity. IBM X-Force Research found that data breaches in the financial services sector increased 937% year-on-year from 2015 to 2016. Of these breaches, 53% were inadvertently caused by employees, often through falling for multiple phishing scams which allowed malware to be installed.

DATA BREACHES

Under GDPR you will need to report data breaches within 72 hours, and prove due diligence in preventing them. You only have to notify your supervising authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly. Clear responsibilities and dress rehearsals for data breaches will avoid fines.

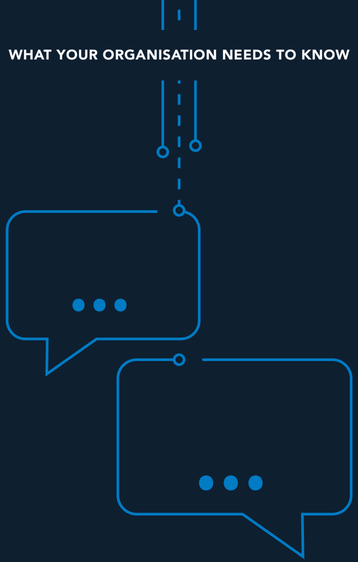
GDPR ROADMAP

6 External Engagement

Once you have revised your data protection processes and responsibilities you can start to communicate them externally with confidence.

The first step in this process will generally be to contact your supervisory authority. For multinational organizations you should map out where your organisation makes its most significant decisions about data processing activities in Europe. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

Your revised processes will need to be shared with all data processing partners. Finally, any revised consent forms and privacy notices should be communicated to the key target audiences, the data owners. If conducted correctly, this should be a positive opportunity to strengthen relationships with customers or employees by demonstrating how seriously you take their data protection rights.



PLAIN LANGUAGE

Remember that all customer communications under the GDPR have to be understandable and non-technical. This includes communications with children.

GDPR CHECKLIST

1. Internal Engagement	×	✓
1.1 Board Commitment		
2. Audits		
2.1 Data Audit		
2.2 Partner Audit		
2.3 Device Audit		
2.4 Privacy Notices Audit		
2.5 Consent Process Audit		
3. Design		
3.1 Revised Policy & Process Design		
3.2 Implementation Plan/Resourcing		
3.3 Compliance Tracker Roll-out		
3.4 Data Portability Procedure		
3.5 PIA Review		

4. Access Definition	×	✓
4.1 Administrative privileges		
4.2 Tiered access		
4.3 Remote access rights		
5. Capacity Building		
5.1 Data Protection Officer Role		
5.2 Training		
5.3 Data Breach Notification Process		
6. External Engagement		
6.1 External Engagement		
6.2 Data Processor Alignment		
6.3 GDPR alignment with data owners		

CONCLUSION: DESIGN WELL, COMMUNICATE OFTEN

The challenges of GDPR may seem daunting, but as mentioned in previous EvoSwitch blogs on the subject (see Sources & Further Reading below) the objectives of the new regulation should be the same as those of any responsible organisation, namely responsible data governance.

GDPR requires thoughtful and flexible ICT infrastructure design. Sensitive data can be protected via a hybrid cloud model and held in a private cloud. At the same time large amounts of data will have to be shared with an increasing number of third party service providers over a wide geographic area. Selection of CSPs based on their compliance and responsiveness should be a key part of your organisation's data protection strategy, and requires an expanded skillset (policy, audit and threat analysis, SLA definition, compliance assessment, and monitoring). You should ensure a broad choice of CSPs so that you are not tied to poorer performers, and this will require a neutral, flexible and continually growing interconnection platform such as EvoSwitch OpenCloud.

Key to successful data management is good quality communication and trust – between the Board and IT departments, between the IT department and all employees, and between the organisation, its partners and service providers, and the people that entrust it with their personal data.

SOURCES & FURTHER READING

Full English text of GDPR:
https://gdpr-info.eu/

Full list of national data protection authorities:
http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

Gartner on delays in compliance:
https://www.gartner.com/newsroom/id/3701117

EVOSWITCH SECURITY BLOGS:
EB:
https://evoswitch.com/blog-security-crossroads-way-now/
EB:
https://evoswitch.com/blog-evoswitch-data-protection/

Symantec 'shadow SaaS solutions' study:
https://www.metasaas.com/blog/the-1-biggest-risk-to-cios

Business Insider on IBM study of financial services data breaches:
http://uk.businessinsider.com/bank-data-breaches-are-up-and-its-an-insider-job-2017-5

Detailed guidance on Consent ICO (UK):
https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

ICO Guidance on data Protection Impact Assessments (UK):
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

UKFast white paper/mythbuster (UK):
http://pdf.ukfast.co.uk/Whitepaper/gdpr_wpaper.pdf

10 steps from the Dutch DPA (NL):
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf

Useful 13 point ICO checklist (UK):
https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

Colophon

Text
The Communication Matrix Ltd
Sander Deutekom
Patrick van der Wilt
Eric Boonstra

Date of publication
December 22, 2017

Design
Studio Piraat