GDPR is a game changer
Are you ready?

Revised and updated

axial™

Introduction

For the past few years, a regulation has been plaguing the minds of businesses everywhere; EU General Data Protection Regulation (GDPR).

Now almost three years later we know what the regulation will be and when it will come into effect (25 May 2018). With the 2018 date looming ever closer, this booklet contains a list of some of our top tips to help businesses prepare.

It should be noted that these tips are not a complete list of everything that should be done but what we believe are the key factors to be aware of in a GDPR project.

Axial Systems understands that the GDPR covers a wide variety of topics - not just security and technology, hence we offer impartial advice and guidance in ensuring your security systems are robust and capable of meeting recommendations.

Contents

25 May 2018

Understand your Data

Document what personal data you hold, where it came from, who has access to it and who you share it with. This means you will need to perform an organisational information audit to ensure controls and practices are being enforced correctly.

For example, if you hold inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so that they can correct their own records. You won't be able to do this unless you have documented what personal data you hold, where it came from and who you share it with.

This documentation process will also help you comply with the GDPR's accountability principle. This requires organisations to show ***how*** they comply with the data protection principles, such as having effective policies and procedures in place.

Privacy by Design

The GDPR places accountability requirements on data controllers to demonstrate compliance.
They need to:

- maintain required documentation;
- conduct a Data Protection Impact Assessment for more risky processing (DPIAs should compile lists of what is caught);
- implement data protection by design and by default, for example, data minimisation.

This means that any new process or system that is implemented into an organisation will need to be checked to ensure it meets privacy by design measures. This will put accountability on organisations to prove that during each phase from evaluation to testing and finally implementation of a new service or system, the GDPR requirements were taken into account and documented. In the event of a breach, this documentation will form the backbone of proof to show that privacy by design was followed at every step.

25 May 2018

Review your Privacy Notices

Currently, when collecting personal data, you have to give subjects certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice.

Under the GDPR there are some additional responsibilities you will need to be mindful of. You must:

- explain your legal basis for processing the data;
- inform subjects of your data retention periods;
- ensure subjects know they have the right to complain to the Information Commissioner's Office (ICO) if they think there is a problem with the way you are handling their data.

In summary, you should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. Note that the GDPR requires the information to be provided in clear, concise and easy to understand language.

25 May 2018

Update your Subject Access Request

The rules for dealing with subject access requests will change under the GDPR. You will need to update your procedures and plan how you will handle requests within the new, shorter time-scales and provide any additional information.

In most cases you will not be able to charge for complying with a request and normally you will have just a month to comply, rather than the current 40 days. There will be different grounds for refusing to comply with subject access requests – manifestly unfounded or excessive requests can be charged for or refused. If you want to refuse a request, you will need to have policies and procedures in place to demonstrate why the request meets these refusal criteria.

You will also need to provide some additional information to people making requests, such as your data retention periods and the right to have inaccurate data corrected. If your organisation handles a large number of access requests, the impact of the changes could be considerable, so the logistical implications of having to deal with requests more quickly and provide additional information will need thinking through carefully.

Transfer Rights

The GDPR imposes restrictions on the transfer of data outside the European Union, to countries or organisations, in order to ensure that the level of protection of subjects data remains the same. This does not mean that data cannot be transferred out of the EU, but any personal data may only be transferred if the controllers are able to comply with the conditions for transfer set out in Chapter 5 of the GDPR. (www.eugdpr.org)

These compliance conditions include the following safeguards:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission.

Right to Erasure

One of the biggest introductions to the GDPR is the "right to erasure". This gives subjects the right to request that their data be removed, under specific circumstances. This does not give subjects the "right to be forgotten" outright, but prevents the business from processing data under the following circumstances:

- the personal data is no longer necessary in relation to the purpose for which it was originally collected/ processed;
- when the individual withdraws consent;
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- the personal data was unlawfully processed (i.e. otherwise in breach of the GDPR);
- the personal data has to be erased in order to comply with a legal obligation;

This also applies to any third party you have shared data with. If you have disclosed the personal data in question to third parties, you must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

25 May 2018

Protect the Crown Jewels

Once you have completed steps 'a-f' it is safe to say that you will have a good grasp of the data you hold and where it is. The next key priority is ensuring that the data is secure in the event of a breach.

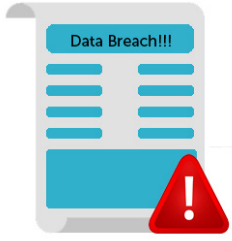
Article 32 states that, data controllers and processors are required to *'implement appropriate technical and organisational measures'* taking into account *'the state of the art and the costs of implementation'* and *'the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.'* (www.eugdpr.org)

The GDPR provides specific suggestions for what kinds of security actions might be considered *'appropriate to the risk,'* including:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

25 May 2018

Set up Data Breach Response Procedures



Some organisations are already required to notify the ICO (Information Commissioners Office), and possibly some other bodies when they suffer a personal data breach. However, the GDPR will bring in a breach notification duty across the board within 72 hours of discovery. This will be new to many organisations.

You should immediately begin making sure you have the right procedures in place to detect, report and investigate a personal data breach. This could involve assessing the types of data you hold and documenting which ones would fall within the notification requirements if there was a breach.

In some cases, you will have to directly notify the subjects whose data has been subject to the breach, especially, where the breach might leave them open to financial loss. Larger organisations will need to develop policies and procedures for managing data breaches – whether at a central or local level.

Note: that a failure to *report* a breach when required to do so could result in a fine, in addition to a fine for the breach itself.

25 May 2018

Provide Evidence

It is important to note that having tools to undertake points 'a-h', is not enough – the regulation requires that you also provide evidence that they have been used correctly.

It is imperative that you follow the approved code of conduct or an approved certification mechanism – as described in the GDPR Article 40 and Article 42 – on how to use these tools to demonstrate compliance with the GDPR's security standards. (www.eugdpr.org)

These codes of conduct or certification mechanisms are designed to ensure that in the event of a breach the business has taken every possible measure to mitigate risk to the data subjects. This evidence will also be important in the discovery of a breach, to identify if the data affected is 'personal data' as outlined in the regulation, as only breaches of this nature need to be reported.

About Axial

Axial Systems is one of the UK's leading solution providers and systems integrators of network, security and services. With an enviable reputation for bringing innovative technologies to the UK market, we have been successfully meeting and exceeding our customers' expectations since 1989 through consultancy, by deploying and managing high-performance network and security solutions, coupled with accompanying managed and support services. Our expert knowledge ensures that our customers challenging current and future business goals are completely met.

Our expertise in both Network/Security Optimisation and Data Security, means that Axial can help you through all stages of optimising your Security and Defence. Visit **www.axialgdpr.co.uk** to find further information around topics related to the GDPR and Security; these will help you become more informed and prepared.

Further information on Axial Systems' portfolio of solutions and examples of how we have applied technology to help customers in blue-chip financial institutions, legal firms, wired and wireless service providers, along with public sector organisations ranging from NHS trusts, education establishments, "blue-light" emergency services and regional and central government, can be found at www.axial.co.uk.