Axxsys Consulting:

Guide to GDPR Compliance

axxsys

Contents

€20 million in fines or up to **4%** of your company's total worldwide revenue*, if you fail to comply

Scope

In May 2018, new laws on data protection and privacy come into force but the Information Commissioner's Office (ICO) has warned that the General Data Protection Regulation (GDPR) is still not on the agendas of senior management at many organisations.

This is a potential disaster for financial services managers struggling to protect their brand and preserve their bottom line in an industry where reputational damage and regulatory fines have been a consistent theme.

The window of opportunity for compliance with GDPR is closing rapidly and the regulation is wide-ranging. The regulatory imperative of GDPR creates some very specific issues for financial services organisations. The cost of non-compliance will be very high, both in terms of the fines and penalties potentially due and the broader reputational damage.

The aim of GDPR is to protect the personal data of EU citizens and enhance legal rights in this area. All firms that deal with EU citizens, regardless of where they are based, must comply and substantial fines can be imposed on those who breach compliance.

GDPR requires financial services organisations to obtain consent for collecting personal data such as email addresses. They need to be specific about how personal data is collected and used, how they allow clients to access this data and how they will correct and delete data if requested.

Penalties

Any organisation found to be in breach of GDPR can be fined up to 4% of global turnover or €20 million whichever is greater for serious infringements of the regulation*. There is also a tiered approach to penalties in place for less serious infringements.

It should be noted that these rules apply to both data controllers and processors.

GDPR Main Changes

The following points provide financial services organisations an indicator to the scale of change that is required for GDPR compliance:

- Does the organisation collect, store and/or process the personal information of data subjects who reside in the EU?
- Does the organisation inform data subjects about the data they are collecting and its purpose?
- How long is the organisation going to keep personal information?
- Can the organisation respond to a request from data subjects for deletion or access to their personal information within 30 days?
- Has the organisation implemented sufficient controls to ensure the confidentiality and integrity of data procession systems and personal information?

Appoint a Data Protection Officer

A Data Protection Officer (DPO) will need to be appointed for any financial services organisation that carries out the regular and systematic monitoring of individuals on a 'large scale. Currently there is no definition of what 'large scale' means; however examples could be processing customer data by an insurance company, wealth manager or bank, or processing personal data for behavioural advertising by a search engine.

The role of the DPO is to help what the GDPR describes as data 'Controllers' and 'Processors' comply with data protection law and avoid the risks that organisations face when processing personal data.

GDPR specifies that this person need not be an employee of the organisation and need not be available on a full time basis but should be involved in all cases where data processing is modified, assessed or implemented.

The DPO should have the following skill sets:

- Expertise in national and European data protection laws and practices
- An in-depth understanding of GDPR
- Understanding of data processing operations and data security
- Knowledge of the relevant business sector to the organisation
- Good communication skills. The DPO will be the public face of the organisation to the Information Commissioner's Office and the public
- Ability to promote a data protection culture within the organisation

Complete a Data Audit / Data Protection Impact Assessment

A full data audit is necessary. This will enable financial services organisations to identify what data they hold, where it is, why they hold it and who has access to it.

In scenarios where data processing is likely to result in a high level of risk to the data subject's rights, the GDPR mandates that data controllers perform a Data Protection Impact Assessment (DPIA). Well prepared organisations, or even those who have already been through risk assessment programmes in the past, may be able to transfer most of this information from their existing risk registers.

Note the ICO has the legal entitlement to request this documentation from any organisation whose business is conducted in their jurisdiction.

Only hold the Data the Organisation Needs

GDPR specifies that data subjects should be made aware, in clear language, why their personal data is being collected, for what purpose and how long it will be stored. Data subjects must explicitly opt-in and accept these conditions with the burden of proof now being placed on the collector.

"There's a lot in the GDPR you'll recognise from the current law, but make no mistake, this one's a game changer for everyone."

Source: Information Commissioner, Elizabeth Denham, January 2017

Axxsys Consulting can help review all points of data collection, including paper based forms, as the GDPR covers anything which becomes part of a filing system in an automated system.

Consider the Purpose of Data Collection

GDPR makes no exception when it comes to the boundaries of what is and what isn't acceptable when collecting personal data. Financial services organisations are legally required to justify why each item of personal data is collected and to collect no more than what is required. Personal data that has been collected can only be held for the length of time for which it is needed, with indefinite not being an option.

Axxsys Consulting can help liaise with the various departments of the financial services organisation to understand what personal data has been collected, whether or not it is strictly required, how personal data is processed for deletion and whether the data carries an expiration date.

Understand Data Subjects Rights

Data subjects have a right to request access to personal data related to them which financial services organisations are storing or processing. The time frame to comply has been reduced from 40 to 30 days and administration fees have been abolished.

Implement the "Right to be forgotten"

Under GDPR the data subject now has the right to be forgotten which entitles the data subject to have the data controller erase their personal data, cease further dissemination of the data and potentially have third parties halt processing of the data.

The conditions for erasure include the data held no longer being relevant for the original purposes for which it was collected for processing, or a data subject withdrawing their consent for the data to be used.

Axxsys Consulting can help setup workflow functions to be easily accessible to data subjects in a manner similar to the way in which they submitted their personal data.

'Axxsys can help set up an exported format which can be read by any other controller, or can provide an automated means of transferring data between controllers without the data subject being an intermediary.'

Consider any Data Sharing arrangements

If a financial services organisation shares clients' data with third parties it must ensure that they have their clients' consent, that the clients' know what the data is being used for and that the firms sharing the data are protecting the data correctly.

GDPR also requires financial services data controllers to provide data subjects with the means to move their personal data between controllers.

Ensure Transparency

A key aim of GDPR is to give people control over their own data, which means companies using the data must provide access on request.

Financial services organisations must be transparent about how and where they store data and the procedure by which it can be accessed.

Security by Design

GDPR tries to alleviate against controls being implemented post-incident and focuses instead on prevention by default. For example, using third party software

Axxsys Consulting can help setup encryption or data masking on non encrypted databases to prevent them being readable to unauthorised parties.

Create or Refine Reactive Policies

GDPR requires the disclosure of breaches to the ICO within 72 hours of the data controller becoming aware. In the most severe cases the data controller is compelled to notify the data subjects individually with information such as what the incident is, which personal data items are affected and how the controller proposes to address the incident.

Axxsys Consulting can help ensure policies and processes are implemented for such scenarios with contact information of the ICO, sufficient logging, investigation tools and template messaging for both the ICO and the data subject.

Ensure that Management is involved and has approved the Project

Success requires that management is involved and committed. Management must commit to plan, implement, monitor, review, maintain and continually improve the management system.

Management should also ensure that resources are available to work with the security management system and that the employees responsible for developing, implementing and maintaining the system have the necessary competence and receive appropriate training.

With these prerequisites in place, Axxsys Consulting can help management:

- Develop a security policy
- Determine objectives and plans relating to security
- Define and allocate roles and responsibilities within security

Axxsys™ Regulatory Practice

We help investment management businesses understand and meet the regulatory challenges they face. Axxsys' operational expertise and long track record of working with the buy-side community are supported by our strong regulatory network and long-standing relationships with trade repositories, system vendors, clearing houses and ARMs. As a result, our technical specialists are uniquely placed to see regulation from the point of view of the client business, providing tailor-made solutions that manage regulatory risk and create value within the operating model.

Contact Information

+44 (0)20 7526 4900
info@axxsysconsulting.com
www.axxsysconsulting.com

New Broad Street House,
35 New Broad Street,
London,
EC2M 1NH,
United Kingdom

+44 (0)20 7526 4900

First Canadian Place,
100 King Street West,
Suite 5700, Toronto,
ON M5X 1C7,
Canada

+1 416 915 4186

616 Corporate Way,
Suite 2-4684,
Valley Cottage,
NY 10989,
United States

+1 845 459 2626

Fax: +44 (0) 20 7526 4901

axxsysconsulting.com

info@axxsysconsulting.com