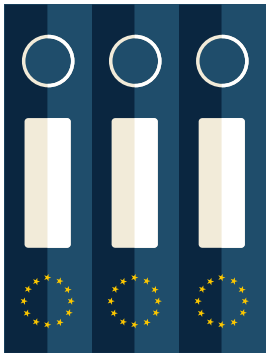
FOURSYS

WHITEPAPER

The IT Manager's guide to GDPR Readiness

Generate a specific Team IT strategy for your GDPR compliance journey covering staffing requirements, conducting reviews, change management and internal communication & training.

If you're reading this document, you'll realise that the EU's new GDPR (General Data Protection Framework) is soon to be in full force.



In actuality, GDPR has been in force since May 25th 2016, and though it will only come into official use on May 25th 2018, it's so far reaching that most organisations are already taking the necessary steps towards compliance.

This legislation is very different to previous rules and regulations requiring organisations to comply with data compliance rules. In contrast, it requires data protection compliance to be embedded specifically and "by design" into the substance of every organisation's processes, procedures, policies and products or services.

These changes are starting to send ripples and waves – even tsunamis – through the corporate and public sector boardrooms up and down the UK.

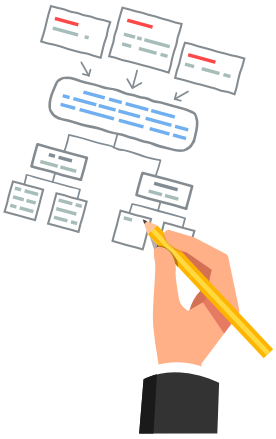
If you haven't done so already, it's now time to start getting up to speed and ready to comply with GDPR.

In this Foursys White Paper, we provide you with an insightful guide to GDPR readiness for 'Team IT'.

Read on to discover the first steps you need to start taking to get your project underway, including:

- Planning your staffing requirements
- Conducting internal reviews to document change requirements
- Implementing the required changes
- Undertaking internal communications and training ahead of readiness

Research and planning



If you've not done it already, your first step is to get to know GDPR inside out.

For starters, make it your business to understand the legal grounds on which your organisation collects and uses data, specifically, aspects of "consent".

How you seek and obtain consent from your customers and contacts to hold data, as well as how you communicate your privacy policies relating to it are both vitally important aspects in this process, and must be documented, implemented and recorded as such.

As you start to develop an idea of the scope and scale of the project that lies ahead, you'll realise that if you haven't yet started, the task of getting your organisation into a state of full compliance by May 25th 2018 is going to be no easy undertaking.

You'll need to develop an understanding of your organisation's stance on GDPR, and the extent to which the requirements of the new regulatory framework are currently understood by senior level executives.

GDPR compliance must be sponsored from the top. Your board need to understand that compliance with the new GDPR regulation will require data protection to be 'designed into' the organisation's systems, policies, processes, products, services and culture from root to branch.

Achieving a state of total compliance is going involve a significant upheaval for some organisations. You and your Board need to be asking the question: "What does GDPR compliance actually look like for us?"

You will need to scope your project plan to include:

- Bringing your senior management team up to speed quickly, if they are not there already
- Assessing the level of understanding for GDPR throughout the rest of your organisation
- Auditing and documenting your current state of GDPR readiness
- Identifying where the gaps exist and the specific measures you will need to take to address them
- Defining the skillsets and other resources you will require to assist you in implementing new systems
- Setting up your internal GDPR Task Force
- Establishing your strategy and project plan to deliver GDPR compliance for your organisation ahead of the deadline

Appointing your GDPR Team

Your internal GDPR Task Force should be a multidisciplinary team with representatives from the key departments and business areas in the organisation that are currently responsible for controlling, holding or processing data.

Additionally, the GDPR framework also stipulates the mandatory appointment of a Data Protection Officer (DPO) for certain types of organisations that manage personal data. This applies regardless of organisation size The DPO can be appointed internally, recruited externally or can be contracted in from a specialist 3rd party organisation.

According to a study by the International Association of Privacy Professionals (IAPP) this requirement means that 28,000 DPOs will need to be hired by organisations in Europe between now and 25th May 2018.

Current thinking is that the following types of organisation will be affected:

- Public sector organisations, bodies and authorities which process personal data
- Any organisation where the core activities consist of large scale data processing operations. Examples may include retailers with online operations and or loyalty schemes
- Any organisation that handles and stores sensitive personal data. Examples may include insurance companies and private medical operators

The role of the DPO is to 'own' data protection within your organisation and to be responsible for everything from informing and advising (through monitoring of regulations), to raising awareness and training of staff and continuous assessment of compliance performance.

When appointing your DPO (or considering sourcing the services from an external specialist), you will need to consider that he/she must:

- Know the whole data protection regulation landscape inside out
- Have the ability to deliver on the core responsibilities of the role
- Be free of internal and external bias or influence in performing the role
- Be credible in dealing with stakeholders at all levels within the organisation, as well as being able to handle

external scrutiny and communications

- Act as the default contact with the office of the Data Protection Commissioner

Conducting Your Internal Status Review

Having defined "What compliance means for us", you will be able to develop your organisation's "GDPR Compliance Profile Checklist".

Kick this off with an internal data discovery exercise (use the Foursys free onsite GDPR data assessment.)

Your GDPR Compliance Profile Checklist should consist of all the 'conditions' which your organisation needs to meet in order to achieve a state of compliance.

You should have representatives on your GDPR Team from all departments and business areas across your organisation that hold and process personal data, you can now task them with:

- Understanding the implications of GDPR on their operational processes
- Assessing and documenting:
  - What personal data they currently hold
  - Where it comes from and how it is gathered
  - The purposes for which the data is held and where it is stored
  - How it is processed, safeguarded, updated and, if appropriate shared
- Listing any specific areas that they feel may put compliance at risk

A key area to assess at this stage is your organisation's privacy information, looking at the consistency of communication and ensuring that you are correctly, clearly and transparently defining your policies.

You should also conduct Data Protection Impact Assessments (DPIA) for riskier activities, for instance where financial information is involved, or where confidential personal details are being supplied. This should identify:

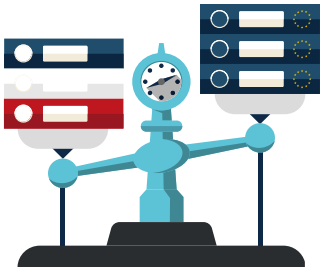
- The data being collected, and whether the methods used to capture, store and manage it are secure and compliant
- The specific risks associated with this higher risk data
- The measures and processes in place to mitigate the risk
- The forms of consent and communication with the contacts

To mitigate the higher risk profile of such data-related activities and review your usage of communications technologies, including encryption, which is instrumental in preventing unauthorised access to sensitive data. This is particularly important with data that is shared electronically within the organisation and with partners.

Among the other provisions of GDPR are requirements for rigorous procedures and policies which should be followed in the event of a data breach.

Your plan should define the internal communications procedures that will come into effect in the event that a data breach is discovered. It should specify the processes that must be set in motion for notifying affected parties and the Information Commissioner's Office (ICO).

Implementing Required Changes



By mid-2017 (at the latest), you should be armed with a documented set of change requirements. Your organisation should be in a position to start making the internal changes, starting with prioritising the areas which represent the most significant data protection risks.

You will be armed with the results of your internal data discovery assessment, a snapshot view of what GDPR compliance will actually look like for your organisation, and a documented set of new and improved processes, policies, procedures and communications.

Externally it's important to ensure that your supply chain and partners are also compliant with the GDPR.

As part of the preparation work, you should contact suppliers with whom you share data, or who process and manage data that you supply to them. This will aid your own GDPR compliance by confirming that their preparations for GDPR are also underway.

If your organisation uses cloud computing, which may involve data storage infrastructure being located outside European borders, you will need to ensure that those contracts are provisioned appropriately for you to be able to meet your GDPR obligations.

Internally, you may also need to review password protocols, verification/ authentication processes, and mobile device (BYOD) policies.

Staff Communication and Training

The person who owns the monitoring and implementation of your organisation's data protection policies is your DPO, the responsibility for communication and training of internal staff should fall within their remit.

The staff who handle, manage and control data will (by late 2017) have no excuse to be oblivious to the changes that are coming. So the objective must be to ensure that all staff understand their own personal responsibilities within the GDPR compliance framework.

They need to understand that the 'accountability principle' of GDPR extends to personal accountability for the controllers, managers and processors of data.

The best way to achieve this is to develop an internal communication and training timetable that aims to reach every member staff, and which:

- Clearly explains the implications of GDPR on the organisation
- Details the exact changes that are being or have been made to data management processes and policies
- Establish guidelines for communications and messaging at all levels of the data lifecycle
- Defines the responsibilities for all staff, and the potential penalties for non-compliance
- Provides guidance for individuals on the steps that they must take in the event that a data breach is discovered

Face to face training can be supplemented with online training and/or personal compliance training.

These communications will carry additional weight if sent out directly by CEO or Managing Director of the organisation.

Summary

It's less than 18 months until the biggest shake-up in data protection, this will require public and private sector organisations around the world that hold data on European citizens to radically rethink the way they safeguard their data.

In a far reaching and long-awaited overhaul to data protection regulations, GDPR will require new unprecedented levels of compliance- with heavy penalties for those in breach of the rules.

GDPR sets out new, broader definitions about what constitutes personal data. It defines what measures the organisations that capture, hold, manage, process and share data must take to safeguard its security. It mandates the appointment of a Data Protection Officer for certain types of organisation and privacy impact assessments where a risk of privacy breach may be high. It also provides for strict new data rights for citizens, including privacy and the 'right to be forgotten'.

The time to start preparing your GDPR readiness plan is now, to ensure the IT department is up to speed and ready for May 2018.

See Foursys's GDPR Timeline Infographic and watch our webinar to find out more about the steps you need to take towards GDPR compliance.

20 Years of IT Security Excellence

For more than two decades, Foursys has operated as a UK-based network security VAR, providing IT security products, services, solutions and support to NHS, government, education, SMB and enterprise organisations. With more than 1,000 customers protecting over 2,500,000 users.

www.foursys.co.uk

Want to find out more?

This guide is designed to give general guidance, however each organisation is unique and we recommend a consultation with a Foursys security specialist if you have any concerns.

Contact us

Main Switchboard

+44 (0)1284 788900

Technical Support

Email

enquiries@foursys.co.uk

Head Office

Manor Park, Great Barton

Bury St Edmunds, Suffolk

www.foursys.co.uk