OryxAlign
taking it personally

EU General Data Protection Regulation

Is your company ready?

GDPR: What you need to know

The Regulation will have a significant impact on businesses, both positive and negative.

- The GDPR will mean a change to operations company-wide, particularly with those in Marketing, HR, Recruitment, and IT who process information uniquely and fit for purpose.
- The first evidence of compliance by organisations and one of the most complex is data consent. The DPA can simply visit a website and sign up to services or newsletters to understand if an organisation is correctly complying.
- Negative Impacts - Cost of implementation, cost of ongoing new processes such as training of staff and monitoring and assessments.
- Positive Impacts - Harmonisation of EU privacy laws, provides opportunity for companies to brand themselves as ethical in the realm of data protection which is a growing concern amongst citizens.
- The Information Commissioner has confirmed that the GDPR will take effect before the UK leaves the EU, and therefore the regulation will apply. It will remain in effect even after our departure for any company who handles the data of anyone present in the EU.
- Nearly one in five (18%) of respondents are worried that non-compliance could ultimately put their organisation out of business[1].

Organisations must act now to ensure that they are ready to comply with the new Regulation when it comes into force in May 2018.

of global companies do not believe they can meet all of the requirements on their own.

Companies can be charged either 4% of their global revenue or €20m, whichever is greater.

Can your company afford to risk non-compliance?

[1] Veritas GDPR Report: https://www.veritas.com/content/dam/Veritas/docs/reports/gdpr-report-en.pdf

Summary of key changes

Fines of up to 4% of annual worldwide turnover	Fines for a breach of the GDPR are substantial. Regulators can impose fines of up to 4% of total annual worldwide turnover or €20,000,000.
Expanded scope	Applies to all organisations involved with the processing of all Personally Identifiable Information (PII) of a citizen within the EU. The definition of this data is also broader, bringing more data into the regulated perimeter including identifiers such as genetic, mental, cultural, and social identities.
Data Protection Officers (DPOs)	DPOs have increased responsibility in compliance and communication and now must be appointed to organisations conducting large-scale systematic monitoring or processing of sensitive data.
Accountability	Organisations must prove they are accountable by: establishing a culture of monitoring, reviewing, and assessing data processing procedures; minimising data processing and retention of data; building in safeguards to data processing activities; documenting data processing policies, procedures, and operations that must be made available to the data protection supervisory authority upon request.
Privacy Impact Assessments	Organisations must undertake Privacy Impact Assessments when conducting risky or large-scale processing of personal data.
Consent	All information pertaining to data processing including purpose, period of time, intent of use, recipients, and withdrawal of consent must be presented to a subject in an easily understood format at the time of data collection. Traditional marketing methods such a silence or pre-ticked boxes are not compliant and all consent records must be kept for proof of compliance.

Controllers and Processors	Organisations must identify their controller and processes and govern them with a new list of responsibilities bound by contractual agreements. This includes ensuring all recipients and authorised persons dealing with the data are under confidentiality or statutory obligation.
Privacy by Design and Default	Organisations should design data protection into the development of business processes and new systems. Privacy settings should be set at a high level by default.
New consumer rights	• The right to be forgotten - the right to ask data controllers to erase all personal data without undue delay in certain circumstances • The right to data portability - where individuals have provided personal data to a service provider, they can require the provider to 'port' the data to another provider, provided this is technically feasible • The right to object to profiling - the right not to be subject to a decision based solely on automated processing
Mandatory breach notification	Supervisory authorities must be notified without undue delay or within 72 hours of awareness of breach when identified as high risk to subjects. Likewise, subjects need to be notified without undue delay in this case.
Subject Access Requests	Access to data must now be free of charge and processed within 1 month unless requests are repetitive or unreasonable.
International transfer of data	New conditions for transferring data outside the EU must be met with 'appropriate safeguards to protect that data and needs to be determined only by approved certification mechanisms.

First steps: Addressing GDPR

1. Awareness

An organisation must raise awareness internally of the new regulations impact to all processes including in HR, Marketing , Recruitment and IT. Sufficient knowledge, resource and commitment of these departments and executives will be required to assess and implement appropriate strategies on the way to compliance. Without co-operation the processes will simply be more difficult, more costly and result in non-compliance by May 2018.

2. Identify sensitive data and where it resides

What data do you hold and process? Analyse all existing data from all sources including databases, PDFs, or other formats and identify its sensitivity through establishing categories and understanding the date it was gathered and consequently the amount of time it's been held for.

How many different locations and environments does the data reside in? This includes detailing geographic locations as well as locations within a data centre or extended data centre (including virtual and cloud environments), and whether data resides on servers (whether file servers, databases, or virtual machines), storage volumes or shares, or disk drives, tapes, or other media.

Where does data get transmitted? This can include data traversing networks between data centres, whether in point-to-point or multi-point environments.

Who has access to this data? Understand what individuals, units, and processes use the data and establish confidentialities, restrictions on persons and tracking methods to ensure full compliance.

How is new data collected? Review your process of collecting this data from the first point of contact with a subject down to their consent and where their consent is stored. It is important that this process is completely compliant with the regulation as it is the first identifier that an organisation may not be compliant.

3. Minimise and structure data sets

You shouldn't be holding any data that is not essential to your service, likewise data older than 15 years will be inaccurate, redundant, and best to be removed. You must minimise exposure by removing all data not required or used.

Furthermore once data locations are identified and understood, it's important to take steps to minimise the number of locations housing sensitive data wherever possible.

Particularly with respect to GDPR, if a business could reduce the number of environments or systems that contain personal data, they could potentially significantly streamline their compliance efforts.

4. Safeguard data leveraging encryption and key management

Encryption represents an essential way to establish data confidentiality and integrity. In fact, the GDPR will only intensify the demand for encryption.

Encryption offers the possibility of obviating the need for breach notification, as required by the GDPR. If a breach occurs but data was encrypted and keys were protected, no one would be able to decrypt the data and access the actual information.

Organisations can ensure that, even if another government issues a subpoena or is secretly accessing a private repository, companies can retain control over who can ultimately decrypt the data.

By deleting a key associated with a consumer's encrypted records, a business could ensure that data will never be accessed in the clear.

5. Control Access

Repeatedly, it is weak, static credentials that are exploited to gain unauthorised access to sensitive resources or perpetuate a full-blown data breach. It is therefore essential for organisations to eliminate this vulnerability by establishing strong, multi-factor authentication to any resource that holds value, be it a network, portal, or application.

6. Look for an experienced partner

Becoming compliant with the GDPR cannot be done alone and organisations should consider a proper assessment of the current data and IT environment to analyse the assistance they need. OryxAlign partner with industry-leading vendors to address the challenges of GDPR compliance head on. Our Enterprise Security Suite is comprised of:

Enterprise Data Security - Vigilant protection, data classification, two-factor authentication, access control, and information loss prevention in a single solution.

Email Management and Archiving - OryxAlign partner with Mimecast to deliver a fully integrated email security, continuity, and archiving cloud-based solution that delivers total end-to-end control of your email, mitigating email risks and reducing the complexity of your mail infrastructure.

Network Security & Threat Intelligence - Cloud-delivered network security and threat intelligence like no other.

OryxAlign
taking it personally

For more information as to how OryxAlign can help your company get GDPR-ready, take our GDPR Readiness Assessment or speak to us about how we can help keep your data safe and secure, regardless of the countries it's being transmitted to.

OryxAlign offers a complete portfolio of enterprise security solutions, enabling our customers to enjoy industry-leading protection. We provide world-class protection across numerous verticals including major financial institutions, real estate, and government bodies.

We help our customers achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect our customers.


MANAGED IT SERVICES


CLOUD SERVICES


ENTERPRISE SECURITY


TECHNOLOGY SOLUTIONS


BUSINESS CONNECTIVITY

OryxAlign, The Shepherds Building, Charecroft Way, London W14 0EH
+44 207 605 7890 | hello@oryxalign.com | www.oryxalign.com