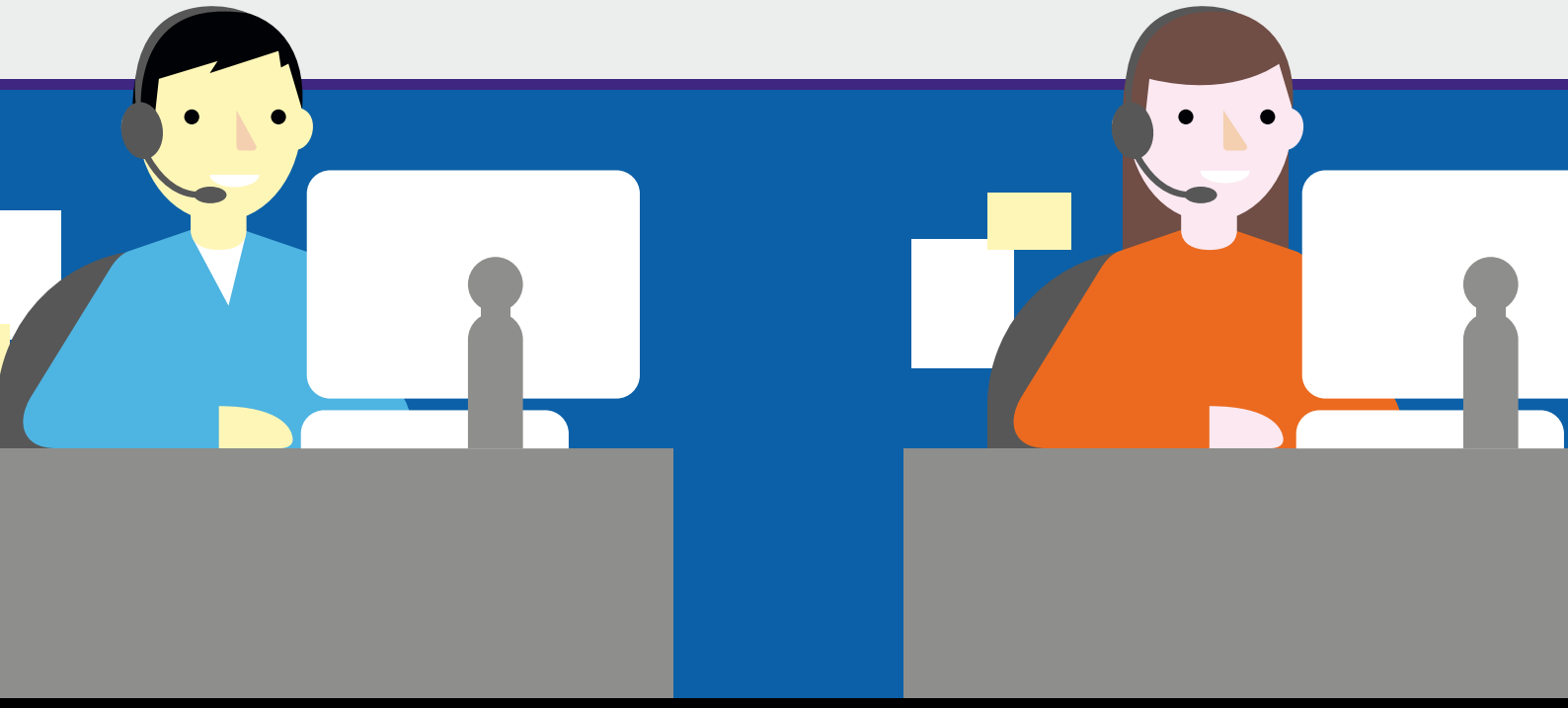
GDPR: the countdown has started

From 25 May 2018, the EU General Data Protection Regulation (GDPR) will affect every organisation that processes EU residents' personally identifiable data.

It is imperative that businesses begin planning now.

- **What exactly is GDPR**
- **Helping you understand the changes**
- **The questions you need to ask**
- **The steps you need to take to get GDPR ready**
- **How we can help you get GDPR ready**
- **Where does Privacy Shield fit into the data protection puzzle**



orange™ Business Services

Introduction

Data protection has always been a contentious issue – but the new EU General Data Protection Regulation (GDPR) will be the most far reaching legislation yet in governing the security and management of both customer and staff personal data – and it will have teeth.

GDPR underlines the privacy of personal data placing significant and far-reaching obligations on businesses, with regard to the way data is collected, processed, and managed.

The regulation will demand that enterprises get a true picture of their IT estate and know exactly where all their data is. Data processors will have to make sure that personal data moved or processed outside the EU, such as in US data centers or the cloud, comply with GDPR. If this turns out not to be the case, this will immediately put up a red flag.

The GDPR puts severe limitations on entities covered by the regulation transferring personal data to recipients outside the European Economic Area (EEA) which is ring fenced as the EU member states, together three members of the European Free Trade Association (EFTA) – Norway, Liechtenstein and Iceland. Where cloud services are using servers or storage, for example, outside the EEA, that are unidentified to the controller or processor, or cloud data processing technology in the EEA is remotely serviced by non-EU providers, it must comply fully with GDPR data transfer regulations.

But there is a silver lining. Creating a single, harmonized level of regulation and compliance across the EU will offer a trusted market for cloud and innovative IT enabled business models providing robust and secure offerings that meet GDPR compliance.

Creating a single, harmonized level of regulation and compliance across the EU will offer a trusted market for cloud and innovative IT enabled business models.

Introduction

The GDPR will have far reaching consequences for both cloud-consuming enterprises, cloud vendors, IT and associated security teams.

The countdown to GDPR has started. Are you prepared?

After many years of planning, GDPR will be enforced from May 2018. It is imperative enterprises prepare now for the new data protection laws or risk getting caught out. Unlike previous Data Privacy obligations, there will be severe penalties for non-compliance or any failures.

As enterprises take action to comply with GDPR, they will find that cloud is one of the most difficult areas. Why? Because this data is processed in many ways – via enterprise data systems and pre-approved cloud services as well as through unstructured avenues such as through collaboration and productivity tools which have been set up by departments or individual employees.

But under GDPR, one must never forget that the enterprise is legally responsible for protecting all data, including unstructured data from alteration, loss or unauthorized processing, even if employees are using cloud services that is not sanctioned or approved by the IT department.

Knowing exactly which personal data is being processed by users of cloud services, identifying which cloud applications are being used by employees, preventing data from being stored or processed in uncontrolled cloud services as well as protecting personal data stored or processed in the cloud will be crucial to being fully prepared for GDPR – and for many will be a large and formidable task.

The GDPR will have far reaching consequences for both cloud-consuming enterprises, cloud vendors, IT and associated security teams. Which is all the more reason to get ahead of the curve and get ‘GDPR ready’ early.

What is the GDPR?

The GDPR, designed to replace the previous Data Protection Directive. It has been created to strengthen and unify data protection for individuals within the EU, whilst addressing the export of personal data outside the EU.

The European Data Protection Regulation will harmonize the current data protection laws in place across the EU member states. The fact that it is a “regulation” instead of a “directive” is key – it means it will be directly applicable to all 28 EU member states without a need for each country to implement its own version of the legislation.

> **‘The fact that it is a “regulation” instead of a “directive” is key’**

GDPR will strengthen and unify data protection for those within the EU and address the export of personal data outside the EU. At the same time the regulation will give citizens back control of their personal data and simplify the regulatory environment for international business by unifying the regulation within the EU.

The GDPR will have far reaching consequences for both cloud-consuming enterprises, cloud vendors, IT and associated security teams who will need to work hard to get their ‘house in order’ in two-year grace period before penalties for non-compliance come into force.

Scope of GDPR

For the first time, GDPR regulates data processors, rather than just data controllers. In GDPR, data processors will have direct legal obligations in respect of the personal data they process. Data subjects (citizen) will be able to claim compensation for unlawful processing of their personal data direct from the processor ie. the datacenter or cloud service operator.

Data processors will be liable to sanctions at the same level as controllers if they fail to meet criteria as set out in the regulation. Where a controller processes personal data jointly with another controller, they can be jointly liable towards a person.

The ramifications of these changes are far reaching. Third parties will need to be on guard when it comes to securing data for others. Data owners will need to screen their partners carefully. The regulation applies if the data controller or processor (organization) or the data subject (person) is based in the EU. Unlike the current Directive, GDPR also applies to organizations based outside the EU if they process the personal data of EU citizens.

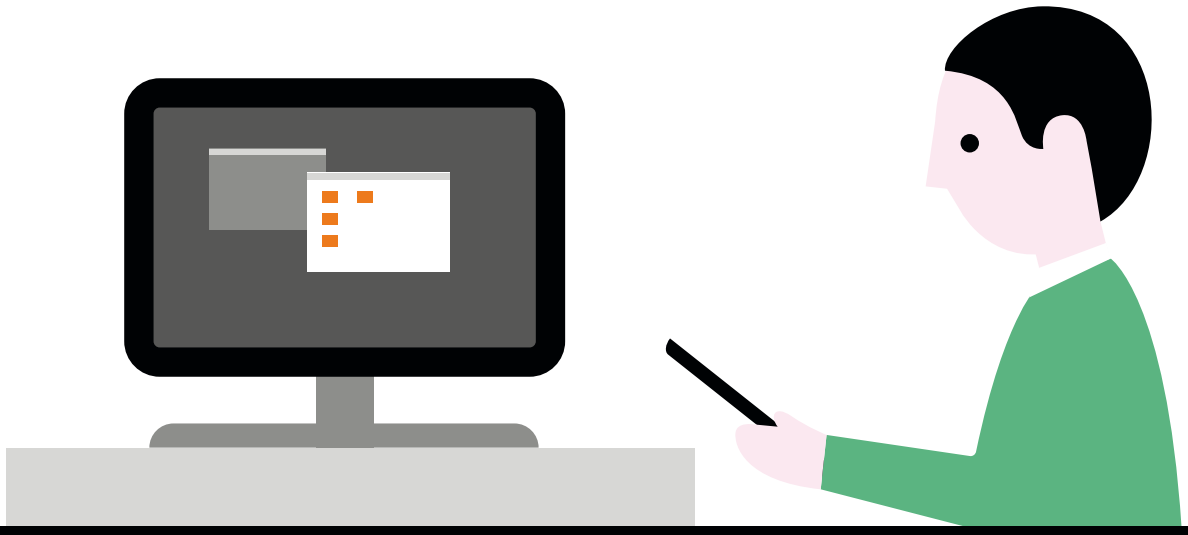
What is the GDPR?

Organisations outside the EU will be subject to the jurisdiction of the EU regulators just by collecting data on EU citizens. Such organisations will only, however, have to work with one single supervisory authority across the EU.

The new Regulation puts much greater emphasis on data security, and enterprises will find themselves subject to tougher security rules, audits and a new data breach notification framework. Data protection authorities, which enforce the GDPR on the territory of its member state, will be able to impose fines of €20 million or up to 4 percent of global annual turnover, whichever is the greater, where businesses are responsible for serious breaches of the regulation. Written warnings can be given in first and non-intentional non-compliance cases and regular periodic data protection audits carried out.

In short this represents a sea-change in risk management for global businesses with harsh repercussions for non-compliance

The new Regulation puts much greater emphasis on data security, and enterprises will find themselves subject to tougher security rules, audits and a new data breach notification framework.



Understanding the changes

Many of GDPR's main concepts and principles are the same as existing legislation in many countries across Europe. But there are also some very different significant elements that may mean you need to change the way you work technically, organizationally and/or culturally. This list outlines some of the key differences you need to familiarize yourself with to make preparations for GDPR.

1. The restrictions on transferring data related to EU citizens will be much stronger. The new regulation will have a much broader territorial scope, applying to non-EU established organizations targeting EU markets by offering their goods, services or monitoring the behaviour of EU citizens. At present, European data protection legislation is only applicable to non-EU controllers if they utilize technology on EU territory to process personal data.
2. The regulation enables users to claim damages if data is lost due to unlawful processing, including collective redress, the EU term defining the legal instrument of group proceedings. Such proceedings can be costly both financially and in terms of reputational damage.
3. Controllers are required to notify the appropriate supervisory authority of a personal data breach within 72 hours if it results in a risk to the consumer. If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay. If there is no risk, the company still has to keep an internal record. Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data is seen as a breach. Mandatory breach notification is not a requirement (under current legislation) in most EU Member States and so this is a significant change to current practice.
4. The regulation places onerous accountability and obligations on data controllers to show that they are compliant. This includes maintaining documentation and carrying out a data protection impact assessment for higher risk data processing functions demonstrating data protection by both design and default.

Controllers are required to notify the appropriate supervisory authority of a personal data breach within 72 hours, if it results in a risk to the consumer.

Understanding the changes

5. The Regulation introduces the concepts of "privacy by design" and "privacy by default". Privacy by design means taking privacy risk into account in designing any new product or service from the onset. Privacy by default means that the collection of any personal data must be fair, lawful and limited to the specified purposes.

> **'Privacy by design means taking privacy risk into account in designing any new product or service from the onset'**

6. A data subject's consent to processing their personal data, either by "a statement or a clear affirmative action" signifies their acceptance to the data being processed. The data controller must be able to demonstrate that consent was given. Existing consent is acceptable if it meets the new GDPR conditions. Withdrawing consent should be possible and easily given. Controllers must inform data subjects of their right to withdraw before consent is given. Once consent is withdrawn, data subjects have the right to have their personal data erased. The importance of "consent" is a key and fundamental principle built into GDPR placing a considerable 'burden of proof' on both processors and controllers.
7. The Regulation underscores a new obligation on the controller to develop "transparent and easily accessible" policies explaining to data subjects exactly how their personal data will be processed, what their individual rights are and how they can be exercised.
8. A higher level of consent is required for the processing of "special categories of personal data". These categories are linked to personal data "particularly sensitive in relation to fundamental rights and freedoms". This includes data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."
9. The GDPR introduces specific protections for children (under the age of 18) by limiting their ability to consent to data processing without parental authorization. Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn. Again, the 'burden of proof' obligation mentioned in point 6 above is applicable
10. Data protection officers must be appointed for all public authorities, and where the main activities of the controller or the processor involve "regular and systematic monitoring of data subjects on a large scale" or where the organization carries out large-scale processing of "special categories of personal data". It requires that they have "expert knowledge of data protection law and practices."
11. A statutory "right to be forgotten" which will allow individuals the right to request a controller to delete data files relating to them if there are no legitimate grounds for retaining them.
12. The regulation introduces a new right to data portability, which allows data subjects the right to receive personal data which has been provided to a controller, in a structured and commonly used and machine-readable format. The data subject can also request data be transmitted directly from one controller to another, if it is technically possible.

The questions you need to ask

It is essential to start planning your approach to GDPR compliance as soon as you can to get 'buy in' from stakeholders and educate staff about the new procedures that may need to be put in place.

The regulation puts greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance will require organisations to review their approach to governance and how they manage data security as a corporate issue. Some sections of GDPR will have greater impact on organizations than others, so it is essential you prioritize them to give them due importance in your planning process.

Here are the key questions you need to ask yourself in preparation for GDPR.

Do you know where your data is?

You should document what personal data you have.

Are your privacy policies up-to-date?

Ensure that all your organization's privacy policies, procedures and documentation are valid and in-order. Data protection authorities can request to see these at any time.

Do you need a data protection officer?

Data protection officers will have to be appointed for all public authorities or where the core activities of the controller involve processing large amounts of data or data within "special categories of personal data". If you do not fall into either of these it would be wise to set up a governance group to officiate over the organization's privacy efforts and reporting.

The questions you need to ask

Do you have a breach notification process?

If you don't have a breach notification process in place, you will need to implement one. This is essential as in the case of personal data breaches, data controllers must notify the supervisory authority of a breach no later than 72 hours after becoming aware of it, unless the personal data breach is "unlikely to result in a risk for the rights and freedoms of individuals". If a notification is not made within 72 hours of the data breach, the data controller must give a 'reasoned justification' explaining the reason for the delay.

These provisions will place an administrative burden on both data controllers and data processors. Large enterprises will need to have clear lines of responsibility to ensure that data breaches within the organization itself are identified and dealt with appropriately. Controllers will need to be able to act on reports and notify data subjects if required.

Can you fulfil 'right to be forgotten',' right to erasure' and the 'right to data portability'?

You will need to be able to address all of these, required under the regulation. To ensure that you can adhere to these you need to put a strategy in place that covers data classification, collection, storage, archiving and destruction.

Do you know who your data protection supervisory authority is?

If you operate internationally you will need to know which data protection supervisory authority you come under.

Steps you need to take now to get GDPR ready

Educate

Start raising awareness of GDPR. Education should cascade from the board and senior management down through the departments, so that everyone is au fait with GDPR and its requirements.

Assess

Examine how data is categorized, tiered, accessed internally. Implementing GDPR could have a significant draw on resources, particularly in more complex organizations and in particularly heavily regulated sectors, e.g. financial services, legal, healthcare. Clearly, this is a major issue for the majority of companies with global operations which needs to be incorporated into budgeting and business planning.

The regulation brings in a breach notification duty across the board, which will be very new for many organizations.

Plan

Have bullet-proof plans in place for accountability and auditing. Check how you communicate privacy information, your procedures covering individual's rights, subject access requests, seeking, obtaining and recording consent and, if required, put systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity. At the same time you should also look at the various types of data processing necessary in your organization, identify the legal basis for its requirement and document it. Your organization will also have to explain the legal basis for processing personal data in privacy notices and when answering subject access requests.

Plan for cloud

Organizations need to know which personal data is being processed by users using cloud services, what cloud applications employees are using, prevent personal data from being stored or processed in unmanaged cloud services and ensure personal data is protected when stored or processed in cloud services.

How we can help you get GDPR ready

As a global Information, Communication and Technology services company, Orange Business Services boasts a long and rich heritage (60+ years) in providing reliable, secure services that are compliant with complex Legal and Regulatory frameworks imposed by global and local territories.

Data protection is a key element of our organisation's DNA, firmly established in everything we do. Here, at Orange we have conducted our own review as part of our internal process for becoming GDPR compliant – working to a timetable of deliverables in time for May 2018. Our skills and our own experience in IT services, security technology, cloud services and consultancy all come together to help customers consider the GDPR challenge and how it might affect their choice of cloud or hosting platform.

The growing complexity of IT landscapes, including the use of cloud services, requires that you actively protect all personal data. To comply with GDPR it is essential your organization processes data in a way that is compliant with the regulation.

To comply with GDPR it is essential your organization processes data in a way that is compliant with the regulation.

How we can help you get GDPR ready

We can provide guidance on how to best manage your cloud services, ensuring cloud services are visible and controlled. We can work with you to check each individual architecture or service and support its transfer from a legacy world to one of digital transformation. Using a range of assessment services and tools we can help analyze and understand current data center IT infrastructure, storage and backup systems. With this data we can build intelligence on current systems, legacy architecture, usage patterns, jurisdiction considerations etc that will enable you to effectively plan for refresh and transformation programs.

As a partner, Orange is here to provide assistance with infrastructure reviews, redesign, migration, or transformational changes that maybe required.

Where does Privacy Shield fit into the data protection puzzle?

Privacy Shield is the replacement for Safe Harbour, which was declared invalid by the European Court of Justice (CJEU) in October 2015. The aim of the EU/US Privacy Shield is to protect the personal data of European citizens when it is transferred to US companies and to offer EU citizens a means of redress if US companies breach their obligations. It is being revised by the EU Commission, following feedback from the Article 29 Working Party, made up of data regulators from EU member states.

Privacy Shield requires organizations to respect customer privacy by ensuring that data is compliantly managed, is only used for initiatives the individual gave permission for and is captured on a mutually clear value exchange. Privacy Shield puts the onus on organizations to ensure that EU citizen's data will not be passed on to third parties outside of the US.

When the Article 29 Working Party finally approves the agreement, it could still be nullified by the European Court of Justice. Currently organizations still have to rely on alternatives such as binding corporate rules, standard contractual clauses and best practices set out by the Article 29 Working Party for transatlantic data transfers.

The EU Commission, however, recognizes that Privacy Shield will need to be reviewed again in 2018, once GDPR comes into force.

About Orange Business Services

Orange Business Services, the Orange entity for business, is both a telecommunications operator and IT services company dedicated to businesses in France and around the world. Our 20,000 employees support companies, local government bodies and public sector organizations in every aspect of their digital transformation. This means we're at hand to orchestrate, operate and optimize: mobile and collaborative workspaces; IT and cloud infrastructures; connectivity (fixed and mobile networks, private and hybrid systems); applications for Internet of Things, 360° customer experience and big data analytics – as well as cybersecurity, thanks to our expertise in the protection of information systems and critical infrastructures. More than 2 million businesses in France and 3,000 multinationals place their trust in us. See why at: **orange-business.com** or follow us on Twitter **@orangebusiness.**

Contact us at: **http://www.orange-business.com/en/any-request**

orange™ Business Services

Exceptional Performance in the Cloud. Intel® Xeon® processors.