GDPR
General Data Protection Regulation

What is GDPR?

- The European Union's **General Data Protection Regulation** (GDPR) is the result of four years of work by the European Union to bring data protection legislation into line with new, previously unforeseen ways that data is now used.

- Currently, the UK relies on the Data Protection Act which was issued in 1998, which was enacted following the 1995 European Union Data Protection Directive, but this will be superseded by the new legislation. It introduces tougher fines for non-compliance and breaches, and gives people more say over what companies can do with their data. It also makes data protection rules more or less identical throughout the European Union.

ebiashara.com

Why was the GDPR drafted?

- Firstly, the European Union wants to give people more control over how their personal data is used, bearing in mind that many companies like Facebook and Google swap access to people's data for use of their services. The current legislation was enacted before the internet and cloud technology created new ways of exploiting data, and the GDPR seeks to address that. By strengthening data protection legislation and introducing tougher enforcement measures, the European Union hopes to improve trust in the emerging digital economy.

- Secondly, the European Union wants to give businesses a simpler, clearer legal environment in which to operate, making data protection law identical throughout the single market (the European Union estimates this will save businesses a collective €2.3 billion a year).

When will the GDPR Apply?

- The GDPR will apply in all European Union member states from 25 May 2018. Because GDPR is a regulation, not a directive, the UK does not need to draw up new legislation - instead, it will apply automatically.

- While the overwhelming majority of IT security professionals are aware of GDPR, just under half of them are preparing for its arrival, according to a snap survey of 170 cyber security staff.

- Just 43% are assessing GDPR's impact on their company and changing their practices to stay in step with data protection legislation, Imperva found. While the respondents were mostly US-based, they would still be hit by GDPR if they handle - or contract another firm to handle - European Union citizens' personal data.

- Despite this, nearly a third said they are not preparing for the incoming legislation, and 28% said they were ignorant of any preparations their company might be doing.

Steps Needed to Start GDPR?

- Create Awareness in the company with people such as policy makers.
- Review and document all data processes and security processes within the company.
- Assess the risk in the existing data processing activity using a privacy impact assessment is required to lower the risk.

Steps Needed to Start GDPR?

- Identify needed measures to be taken with the current data processes and apply for any bills that will be needed to achieve compliancy.
- Identify key partners and work with them to create instructions on how data should be handled.
- Review contracts and policies and change where needed to be.

Steps Needed to Start GDPR?

- Check if you are required a data protection officer under the GDPR.
- If you have different areas around the world where you work then consider one has the hub and have the same consistency of the information flowing.
- Inform and enforce any changes to the policy, terms and conditions and contracts to third parties.

Who does the GDPR apply to?

ebiashara.com

- 'Controllers' and 'processors' of data need to abide by the GDPR. A data controller states how and why personal data is processed, while a processor is the party doing the actual processing of the data. So the controller could be any organisation, from a profit-seeking company to a charity or government. A processor could be an IT firm doing the actual data processing.

- Even if controllers and processors are based outside the European Union, the GDPR will still apply to them so long as they're dealing with data belonging to EU residents.

- It's the controller's responsibility to ensure their processor abides by data protection law and processors must themselves abide by rules to maintain records of their processing activities. If processors are involved in a data breach, they are far more liable under GDPR than they were under the Data Protection Act.

When can I process data under the GDPR?

- Once the legislation comes into effect, controllers must ensure personal data is processed lawfully, transparently, and for a specific purpose. Once that purpose is fulfilled and the data is no longer required, it should be deleted.

What do you mean by 'lawful'?

- 'Lawfully' has a range of alternative meanings, not all of which need apply. Firstly, it could be lawful if the subject has consented to their data being processed.

- Alternatively, lawful can mean to comply with a contract or legal obligation; to protect an interest that is "essential for the life of" the subject; if processing the data is in the public interest; or if doing so is in the controller's legitimate interest - such as preventing fraud.

How do I get consent under the GDPR?

- Consent must be an active, affirmative action by the data subject, rather than the passive acceptance under some current models that allow for pre-ticked boxes or opt-outs.

- Controllers must keep a record of how and when an individual gave consent, and that individual may withdraw their consent whenever they want. If your current model for obtaining consent doesn't meet these new rules, you'll have to bring it up to scratch or stop collecting data under that model when the GDPR applies in 2018.

What counts as personal data under the GDPR?

- The European Union has substantially expanded the definition of personal data under the GDPR. To reflect the types of data organisations now collect about people, online identifiers such as IP addresses now qualify as personal data. Other data, like economic, cultural or mental health information, are also considered personally identifiable information.

- Pseudonymised personal data may also be subject to GDPR rules, depending on how easy or hard it is to identify whose data it is.

- Anything that counted as personal data under the Data Protection Act also qualifies as personal data under the GDPR.

When can people access the data we store on them?

ebiashara.com

- People can ask for access at "reasonable intervals", and controllers must generally respond within one month. The GDPR requires that controllers and processors must be transparent about how they collect data, what they do with it, and how they process it, and must be clear (using plain language) in explaining these things to people.
- People have the right to access any information a company holds on them, and the right to know why that data is being processed, how long it's stored for, and who gets to see it. Where possible, data controllers should provide secure, direct access for people to review what information a controller stores about them.
- They can also ask for that data, if incorrect or incomplete, to be rectified whenever they want.

What's the 'right to be forgotten'?

- Individuals also have the right to demand that their data is deleted if it's no longer necessary to the purpose for which it was collected. This is known as the 'right to be forgotten'. Under this rule, they can also demand that their data is erased if they've withdrawn their consent for their data to be collected, or object to the way it is being processed.
- The controller is responsible for telling other organisations (for instance, Google) to delete any links to copies of that data, as well as the copies themselves.

What if they want to move their data elsewhere?

- Controllers must now store people's information in commonly used formats (like CSV files), so that they can move a person's data to another organisation (free of charge) if the person requests it. Controllers must do this within one month.

What fines are there for failing to obey the GDPR?

- Well, if you don't follow the basic principles for processing data, such as consent, ignore individuals' rights over their data, or transfer data to another country, the fines are even worse.
- Your data protection authority could issue a penalty of up to €20 million or 4% of your global annual turnover, whichever is greater.

Advantages of GDPR?

- **Data Volume Reduction –** As the run-in to GDPR commences, the drive to reduce Data volumes will increase, which will in turn vastly reduce the cost and operational inefficiencies associated with keeping masses of redundant and obsolete emails and files on your servers.
- **Data Analysis –** One of the sayings that is prevalent in Waterford Technologies is that "you can't manage what you can't see.." Undertaking the GDPR readiness project will shine a big light on stuff that simply should not be on your servers.
- **Data Retention Policies –** Once the analysis phase of checking what Data is valuable, what can be deleted and what must be retained for compliance purposes (but is not being actively used) is completed, you will set sensible Data Retention policies to manage information in the best possible ways.

Advantages of GDPR?

- **Data Quality –** Data ages very quickly – even records that are mere months old can be completely out of date and storing and sifting through this unstructured Data mess wastes resource time and storage space. GDPR ensures information is only kept as long as it is valid and for the purpose it was gathered.
- **Security** – With Data breaches screaming from the headlines daily, the GDPR will ensure you must adopt better policies with Data under management – benefiting both your reputation and your end users' Data.
- **Trust –** As companies adopt better Data policies to comply with GDPR, the overall trust level between companies dealing with each others' information will rise.

Advantages of GDPR?

- **Future Proofing –** The era of Compliance has begun and more legislation will follow to regulate the sprawl of exponentially growing volumes of Data. Getting a true oversight of your information assets will allow you to set rules to manage your Data properly making you readier for the next legislation.
- **Operational Insight** – The exercise of preparing for GDPR will give good insight into what information departments are holding, why they are holding it and what it is being used for.
- **Big Data Business Intelligence –** Getting everything ready for GDPR will give you a rare opportunity to look across all Data sets and the capability to set up data-centric practices to get insight into running your business better and attracting and keeping more clients.

Disadvantages of GDPR?

- Anybody working in the Compliance and Data Management fields will know a lot about the GDPR legislation by now. It is coming in May, will involve a lot of preparation and there is a really big punitive financial stick of €20 million or 4% of turnover. Compliance legislation can easily be seen as a negative – there is more work, more things to worry about doing the right way and of course, the threat of being found non-compliant can add great stress to already busy managers.

Waterford Technologies Compliance

- Waterford Technologies are experts in data management. Our team consists of expert consultants in Data Protection Legislation, Compliance Technology and Data eDiscovery, Analysis and Investigations.
- We enable organisations to make Data Decisions Based on Fact giving clients a clear overview of their data, enabling informed business decisions to prepare for GDPR. We simplify data oversight by providing cutting edge technology and unlimited unrivalled support.
- To know more about them kindly view the link below.

https://www.waterfordtechnologies.com/

Companies To Be Targeted for GDPR?

- Exporting companies to Europe.
- Importing Companies from Europe.
- British American Tobacco.
- Kenya Buries.
- Finley's.
- Brookband.
- Bamburi Cement.
- Tech Companies.
- Telecommunication Companies.
- Retailers.
- Banks.
- Government.
- Online Shopping Sites.

Enabling GDPR Compliance in Government

- Existing compliance approaches already in alignment with the GDPR provide a good foundation to start from.

- eBiashara will help discover data across your applications, tools and databases.

- eBiashara will help governments limit their exposure to risk by reducing the amount of citizen data they need to process and store, as well as limiting the storage of sensitive data such as passwords.

Enabling GDPR Compliance in Government

- eBiashara provides an Information right management tool to help protect data across its lifecycle by preventing sensitive information from being printed, forwarded, saved, edited, or copied by unauthorized individuals.

- eBiashara will provide a service trust platform which provides access to audit reports and compliance guides to help you understand how you can access and manage the compliance.

- eBiashara has a compliance manager who helps assess and track data protection and compliance posture and get actionable insights to improve. With an intelligence score, customers can better understand their compliance posture against regulatory standards.

Enabling GDPR Compliance in Financial Services

- Existing compliance approaches already in alignment with the GDPR provide a good foundation to start from.

- eBiashara will help discover data across your applications, tools and databases.

- Access Management can help manage access to data across platforms, whether in the cloud, on premise or in a hybrid environment.

Enabling GDPR Compliance in Financial Services

ebiashara.com

- Information rights management helps to protect data across its lifecycle by preventing sensitive information from being printed, forwarded, saved, edited or copied by unauthorized individuals.

- Financial services program provides access to GDPR compliance documents and security experts and auditors.

- Compliance Manager helps assess and track data protection and compliance posture and get actionable insights to improve. With an intelligent score, customers can better understand their compliance posture against regulatory standards.

Enabling GDPR Compliance in Education

ebiashara.com

- eBiashara will help discover data across your applications, tools and databases.
- eBiashara can help identify sensitive data types, enabling you to better understand what sensitive data you have in store.
- Access management can help manage access to data across platforms.

Enabling GDPR Compliance in Education

- eBiashara provides valuable tools such as data encryption to limit exposure to risk, visibility and control over your resources to quickly detect and investigate threats and more.

- eBiashara provides deep visibility into user, device and data activity, helping you protect data – whether its on a faculty's device, stored in a database, shared on class team site, or processed by a cloud app.

- Compliance manager will help assess and track data protection, compliance posture and get actionable insights to improve.

Enabling GDPR Compliance in Health

- Existing compliance approaches already in alignment with the GDPR provide a good foundation to start from.

- eBiashara will help discover patient and health data across your applications, tools and databases.

- Access management will help manage access to data across platforms, whether in the cloud, on premise or in a hybrid environment.

Enabling GDPR Compliance in Health

- eBiashara provides a secure platform to store patient and health data. eBiashara encrypt the data so that to increase security and reduce exposure to risk.

- eBiashara has a service trust platform which provides access to audit reports and compliance guides to help you understand how you can use service features to manage compliance.

- Compliance manager will help assess and track data protection and compliance posture and get actionable insights to improve. With an intelligent score, customers can better understand their compliance posture against regulatory standards.

Enabling GDPR Compliance in Manufacturing

- eBiashara can help identify worker, corporate employee, subcontractor, supplier and customer data automatically held within eBiashara.
- eBiashara will help uncover personal data in your systems, databases, and applications across your entire business – from factories to headquarters.
- Access Management can help manage access to data across platforms, whether in the cloud, on premises or in a hybrid environment.

Enabling GDPR Compliance in Manufacturing

ebiashara.com

- Information rights management help protect data across its lifecycle by preventing sensitive information from being printed, forwarded, saved, edited, or copied by unauthorized individuals.

- eBiashara uses advanced encryption and biometric authentication to secure your employees devices and task specific machines.

- Compliance manager will help assess and track data protection and compliance posture and get actionable insights to improve. With an intelligent score, customers can better understand their compliance posture against regulatory standards.

Enabling GDPR Compliance in Retailers

- Existing compliance approaches already in alignment with the GDPR provide a good foundation to start from.
- eBiashara will help discover data across your applications, tools and databases.
- Access management can help manage access to data across platforms.
- Data masking anonymizes data, enabling you to use the data for analysis.

Enabling GDPR Compliance in Retailers

- eBiashara provides a secure and a platform to store data. We use encryption to increase security and reduce exposure to risk.

- eBiashara employs information rights to protect data from unauthorized access while enabling your sales and store operations teams to connect to the information they need from virtually anywhere.

- eBiashara can help protect kiosks, point of sale, assisted sales devices with threat resistant security features.

Thank you

www.ebiashara.com