NEW

GDPR REGULATIONS 2018

is your business prepared?

S2S GROUP

Providing the **solutions** to corporate data **security**

WHAT IS THE GENERAL DATA PROTECTION REGULATION?

- In response to an increasingly data-driven business environment in a world full of high cyber security risks, new legal frameworks have been put into place in regards to Data Protection, aiming to improve privacy in general and data containment.
- The General Data Protection Regulation (GDPR) is a new enhancement to data protection laws that will come into action **March 25th 2018.**
- Although this may seem a while away yet, it's critical your business is prepared and any changes required aren't left until last minute. GDPR is the most significant change to data protection in the past 20 years and it will impact every organisation that does business in the EU. There is no expectation that the UK's and the decision to leave the EU will affect the commencement of the GDPR.

WHY IS IT SO IMPORTANT?

- In order to maintain data legality within a business, a company must comply with data privacy laws that control how data is stored and distributed. Businesses who do not conform to the new General Data Protection Regulations can be prosecuted and fined a hefty amount. The GDPR applies to any organisation that holds Sensitive or Personal data.
- **What steps does my business need to take?**
- Most organisations are unsure about what GDPR means for their business or what actions they need to take in order to meet the new requirements. Organisations must be able to show how they comply with data protection principles such as having effective policies in place. Here are our 10 steps we think are important to help your business get prepared for GDPR May 2018. For more information, read through this ICO Guide.

STEP 1:
ENSURE ALL DECISION MAKERS ARE MADE AWARE

- The first step is to ensure all key decision makers within your business are made aware of the change within the GDPR law. They should understand the impact of the regulation and check if there are areas of concern that may cause compliance issues once the new law is registered. We advise you to perform a risk assessment early on and follow through with a plan.

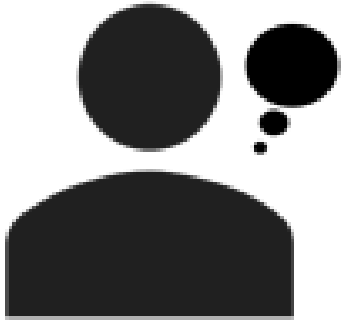
STEP 2:
DOCUMENT ANY INFORMATION YOU HOLD

- You should document all the types of data your business holds, including Personal or Sensitive information. Organise an information audit within your company and understand where your data comes from and who it is shared with. New GDPR regulations require businesses to store records of data processing activities. All inaccurate information must be immediately discussed with any other organisations you may share this data with as all records must be correct.

STEP 3:
COVER ALL INDIVIDUAL'S RIGHTS

- The rights under the GDPR are the same as those under The Data Protection Act but with some enhancements. The right to data portability is a new factor from the GDPR. Ensure that your procedures cover all individual's rights such as the right to be informed, the right to access their data and the right of erasure. Plan who is responsible within your business and how you would act if an individual asks to have their data deleted. Consider making changes if needed.

STEP 4:
REVIEW HOW YOUR COMPANY ASKS FOR CONSENT



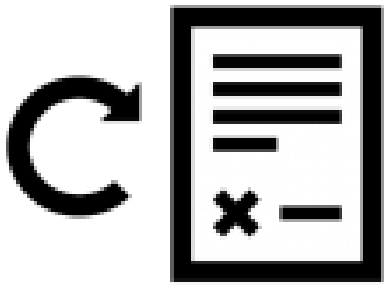
- It’s important that your business reviews how you seek, record and manage consent from data providers so you can update these policies before the GDPR is established next year. Consent must be granted in all cases and an ‘opt-in’ feature must be in place. It must also differ from your Terms and Conditions and data subjects must have access to easily withdraw or change how they consent. Alter your consent policies to meet GDPR regulations or find alternative methods.

STEP 5:
ENSURE YOU HAVE EFFECTIVE PROCEDURES IN PLACE TO DETECT A DATA BREACH

- This is one of the most critical steps on this list. It's important that your business has effective procedures in place to detect, prevent and investigate a data breach. The GDPR has introduced a duty on all organisations that states businesses must report certain types of data breaches to the ICO which includes discrimination, reputational damage and financial loss. If a breach is likely to affect the rights of individuals, those concerned will also have to be notified. Failure to report a breach when required to do so will result in a fine.

STEP 6:
REVIEW YOUR CURRENT PRIVACY NOTICE

- Make sure your business reviews its current privacy notice and be sure to adapt it in time to implement the changes of GDPR. When collecting personal information, your identity should be revealed at all stages along with what your intentions are with the data – this is usually done through a privacy notice. Individuals have the right to inform the ICO if there is a problem in the way you are handling their data.



STEP 7:
UPDATE PLANS FOR SUBJECT ACCESS REQUESTS

- Update your company's procedures and plan how you're going to handle requests, taking new rules into account. If your organisation handles a lot of access requests, it may be a good idea to consider logistical implications of having to deal with requests more efficiently. Consider developing systems to allow individuals to access their data online, ensuring that you are conforming to GDPR and allowing full visibility of client data. Individuals are now required to be informed why their request is rejected without delay, within in the space of a month.

STEP 8:
BE CAREFUL OF COLLECTING CHILDREN'S PERSONAL DATA

- The GDPR will put procedures in place when it comes to protecting children's data online. This is in line with information obtained from commercial internet services and social networking. If your organisation offers these services, you may now need permission from a parent or guardian to collect this sensitive information. According to new regulations, the minimum age at which a child can give consent is at 16, although this may be lowered to the age of 13 in the UK. This could lead to significant complications within your business if you do not comply with these new regulations.

STEP 9:
CARRY OUT DATA PROTECTION IMPACT ASSESMENTS

- The GDPR has made it a legal requirement to adopt a ‘privacy by design approach’ by completing Data Privacy Impact Assessments (DPIA) regularly within your business or organisation. A DPIA is mandatory in situations where data processing is likely to result in a risk to individuals, such as when there is processing on a large scale, when new technology is being deployed and when a profiling operation is likely to affect others. Start assessing situations within your business where it might be necessary to conduct a DPIA.

STEP 10:
DESIGNATE A DATA PROTECTION OFFICER WITHIN YOUR BUSINESS

- Designate someone within your business to become your Data Protection Officer and take responsibility for data protection compliance. GDPR may require you to formally appoint a DPO. This may be the case if you are a public authority, an organisation that monitors individuals on a large scale or if you process special categories of data, such as health or criminal records. The Article Working Party has produced guidance on the duty of Data Protection Officers which can be read here.

NEED FURTHER GUIDANCE?

- If you would like any further guidance on the GDPR or any extra information on how to be GDPR ready, feel free to get in touch with a member of our team. We're always here to answer any queries you may have.

- **Call us on** 01709 878 878

- **Email us at** info@s2s.uk.com

S2S GROUP

Providing the **solutions** to corporate data **security**