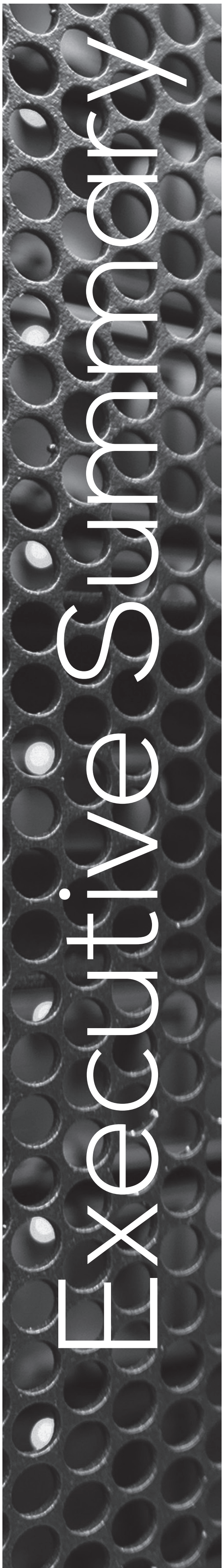


# The General Data Protection Regulation (GDPR)

CAMEO INNOVATIONS

- GDPR is new European data protection legislation that comes into force on May 25 2018
- The UK government has committed to implement the legislation, even after Brexit
- There are major changes from the existing UK Data Protection Act (DPA)
- Its approach is that data will be compromised, so it requires measures to mitigate any impact on an individual of the data breach
- Fines for non-compliance are up to the greater of £8.5m or 2% of global turnover; fines are doubled for an actual data breach
- The definition of “personal data” is extended to include such things as cookies, internet IP addresses and RFID tags; it also includes employee, student and membership data
- It gives individuals several new rights, including the right to be forgotten
- It removes the £10 charge for providing someone with their data (a Subject Access Request or SAR), and reduces the time to supply the data to 30 days
- It applies to almost every business, and it removes any distinction between individual and business data
- Liabilities cannot be passed to a third party even if they are processing the data for you (e.g. third-party credit card processing)


- Security of the data and its secure, encrypted storage, is key, and must be built in to any process
- Presumed consent, silence, continued use, or pre-checked boxes are no longer deemed consent – this probably means obtaining new consent from most existing data subjects
- You are required to document, and be able to prove, conformance
- Some types of data (e.g. employee data or customer data required to supply goods or services) may be processed without consent as the regulation says you have a “legitimate interest” but other requirements, for example, security of data storage, still apply
- New procedures for collecting, storing, and processing data, giving data subjects access to their own data through a portal, and staff training are all recommended or required
- If a data breach occurs you <u>must</u> notify the regulator, in some circumstances the data subjects, and sometimes the public, <u>within 72 hours</u> – so a process to do this has to be designed and put in place in advance
- There’s a lot to do, so you need to start as soon as possible – time is short!

***Next Steps:*** *become better informed, conduct an information audit of what personal data you, and/or your data processor are storing. Identify where it’s stored, how secure it is, whether you need it and whether you have, and can prove, a legal basis to use it.*

**Further information:**

- Cameo Innovations’ GDPR White Paper: cameoinnovations.com/gdprwp
- ICO’s 12 steps to take: bit.ly/ICO_12
- EU Data Protection Working Party’s Guidelines on DPOs: bit.ly/DPO_Guidelines
- White & Case’ Practical Handbook on GDPR: bit.ly/WC_handbook
- Out-law’s GDPR page: bit.ly/OutLawGDPR
- Microsoft’s GDPR information page: bit.ly/MS_GDPR

cameoinnovations.com
+44 20 3745 6111

email: info@cameoinnovations.com
LinkedIn: www.linkedin.com/company/cameo-innovations
Twitter: @cameo_inno