THE NEW GENERAL DATA PROTECTION REGULATIONS COME INTO EFFECT IN MAY 2018

WHAT DOES THE GDPR MEAN FOR MY BUSINESS?

SCOPE

- All EU citizens' personal data falls under the scope of the GDPR, whatever country or jurisdiction this is held in, as well as for any processing outside the EU.
- 'Data subject' definition is widened to include IP addresses, biometrics, photographic images, and anything that can identify a person.
- Suppliers (processors) need to comply with the GDPR.

- **Have you considered the implications of the new definition of personal data?**
- **What steps have you taken to categorise and register all assets, including classes of data held e.g. CCTVs and biometrics?**
- **Have you reviewed contractual agreements with suppliers and confirmed in which countries they hold your data?**

DATA SUBJECT RIGHTS

- Increased rights to: Be Forgotten + Access + Rectify + Transfer + Withdraw + Restrict processing + Object to profiling + Complain.
- By design and by default, data privacy must protect subjects' rights and interests.

- **What data do you hold? Why and where is it held and for how long? Can you justify its being held?**
- **Does your privacy statement explain all rights AND confirm your legitimate interest to process data?**
- **What is your process to answer any data subject access requests free of charge? Can you do so within the mandatory timeframe?**
- **What process and controls do you have around transferring data?**

TRANSPARENCY & USAGE

- All data taken must be explicitly given (opt-in only) or there must be a legitimate interest to process.
- All consent must be unbundled from T&Cs: generic clauses no longer apply.
- Privacy statements must be detailed and clear.

GOVERNANCE

- It is no longer just about doing the right thing: now you must prove it.
- Record all: Processing + Personal Impact Assessments + Breaches.
- Data privacy by design.

- **How have your Board, owners and key staff been made aware of the new legislation?**
- **Do you need and/or have you appointed a Data Protection Officer?**
- **What evidence do you have to prove your compliance to regulators and stakeholders?**
- **What processes and procedures do you have in place to regularly review and test compliance?**

COMPLIANCE

- Mandatory breach reporting within 72 hours of being aware.
- Data Protection Act is now combined with Anti-Bribery and Anti-Trust laws, resulting in new and increased penalties and sanctions.

- **What is your Breach Management Policy?**
- **What is your Incident Management Procedure?**
- **How will you communicate to all stakeholders?**

PROTECTION

- Whether at rest or in transit, data needs to be secure (encryption and pseudonymisation).
- Systems, data access and data usage must be tracked and monitored.

- **How secure is the personal data you hold?**
- **How often do you perform audits?**
- **What accreditations do you have to demonstrate security?**

riskevolves

info@riskevolves.com

www.riskevolves.com | **01926 800710**