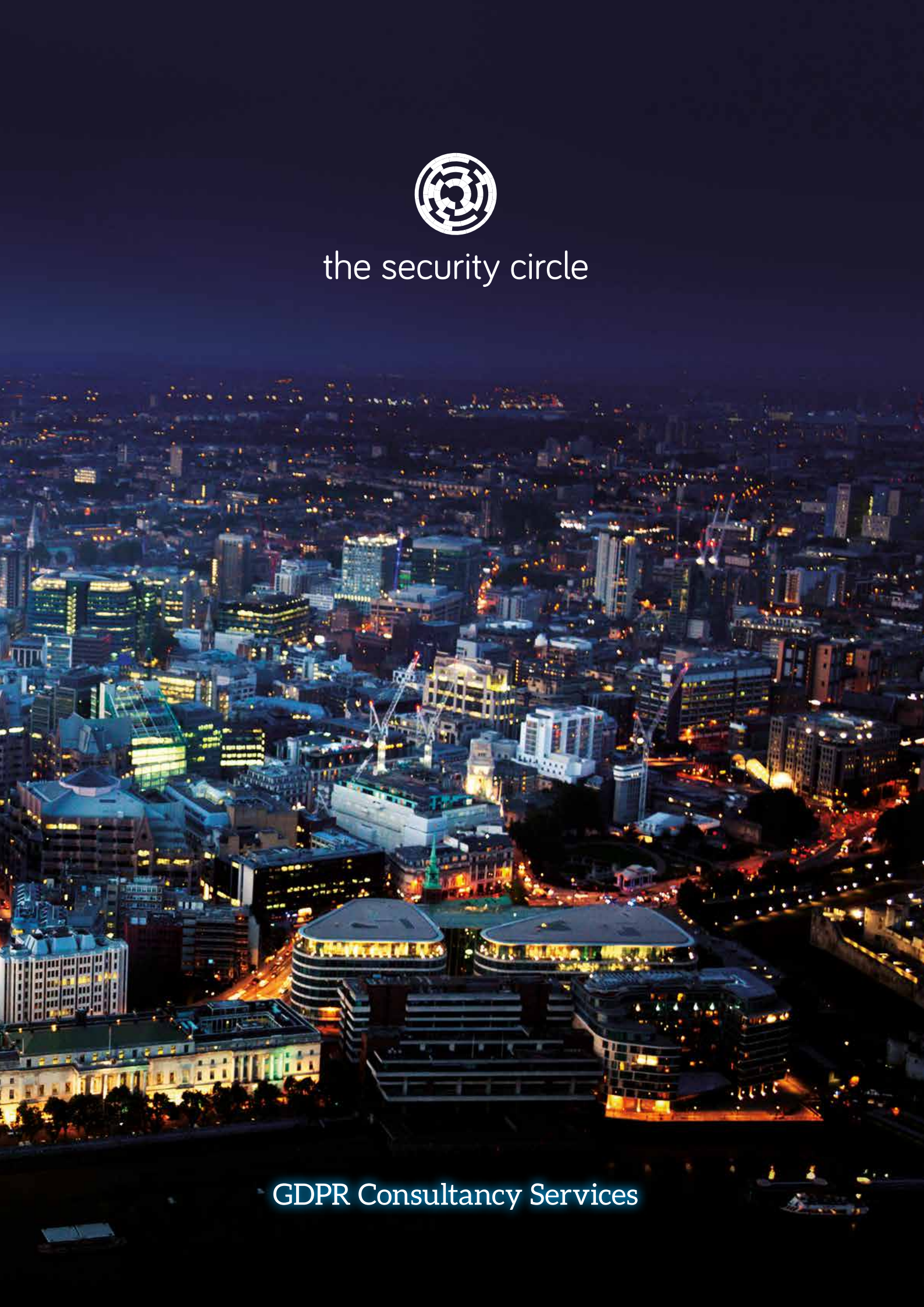
the security circle



GDPR Consultancy Services

Our GDPR Consultancy Services

Information is the 21st Century's global currency and the new GDPR (The General Data Protection Regulation of the EU) places the protection of user information at the heart of any organisation.

As of May 25 2018, the new GDPR is the law if you do business in the EU zone. Amongst other tools an annual audit should provide a measure of security to ensure ongoing adherence. The Security Circle's team of GDPR specialists are on hand to take your business through every stage of the process to becoming GDPR compliant, then subsequently retaining this compliance. The penalties for failing to comply with GDPR are severe - up to 4% of annual global turnover or 20 million Euros, whichever is higher.

The new GDPR is an evolution of the GDPR is an evolution of the EU's existing data rules, the Data Protection Directive (DPD). It addresses many of the shortcomings in the DPD: adding requirements / recommendations fordocumenting IT procedures, performing risk assessments under certain conditions, notifying the consumer and authorities when there is a breach, as well as strengthening rules for data minimisation.

It also addresses export and processing of personal data outside the EU.

One way to describe the GDPR is that it simply provides a legal framework to a lot of common sense data security ideas, especially from the Privacy by Design school of thought: minimise collection of personal data, delete personal data that is no longer necessary, restrict access and secure data through its entire lifecycle.

TOOLS

1. **Privacy by Design (PbD)**
2. **Data Protection Impact Assessments (DPIA)**

KEY ISSUES

3. **Right to Erasure and to be Forgotten**
4. **Extraterritoriality**
5. **Breach Notification**
6. **Fines**

Privacy by Design (PbD) is a fairly long-standing and well-intentioned set of principles. The Security Circle can give you a Guide for this to get the C-suite to take consumer data privacy and security more seriously.

1. Privacy by Design (PbD)

With just a few basic steps, you can achieve the PbD vision:

- Minimise data collected (especially PII) from consumers
- Do not retain personal data beyond its original purpose
- Give consumers access and ownership of their data.

Businesses (and marketers) always want more data - age, income, postcode, favourite films, books, food - even for the simplest consumer interaction. What the GDPR says is that marketers should limit data to the purpose for which it is being collected and not to retain the data beyond the point where it's no longer relevant.

So the data you collected 10 years ago -maybe containing 3000 email address along with a lot of minor personal detail - and now lives in spreadsheet somewhere in the system? Well, you need to find it and delete it.

If a hacker gets hold of it and uses it for phishing purposes, you've created a security risk for your customers. If the local EU authority can trace the breach back to your company, you will face a hefty fine.

It's not too much of a stretch to say that if you implement PbD, you're well on your way to mastering the GDPR.

2. Data Protection Impact Assessments (DPIA)

This is an important tool to assist in conforming with the new regulations. The Regulators may expect to see that you have analysed your risks and the security of your customer's data.

This is where The Security Circle comes in. We can give you analysis sheets to start the process of finding out where and what the gaps are. We keep it light touch and appropriate for the size and risk profile of your business. It is not one size fits all.

3. Right to Erasure and to be Forgotten

For most companies, this is really a right for consumers to erase their data.

There's now direction to force companies to take reasonable steps to inform third parties of a request to have information deleted.

What if the processing company gives the personal data to third-parties, say a cloud-based service for storage or processing?

The long arm of the EU regulations still apply: as data processors, the cloud service will also have to erase the personal data when asked to by the controller.

Translation: the consumer or data subject can request to erase the data held by companies at any time. And that means you have to know what it is and where it is - in EVERY location.

4. Extraterritoriality

The GDPR will apply to any data transferred outside the EU zone. So if a US company collects data from EU citizens, it would be under the same legal obligations as though the company had headquarters in say France, UK, or Germany - even though they don't have any servers or offices there.

It might be hard to enforce but you only have to look at the apps on your phone to see how many companies outside of the EU have your data and are therefore subject to the GDPR laws and penalties. The issue of the USA patriot Act will provide further complications.

5. Breach notification

You have to notify a breach inside 72 hours. If that happens on a Friday at 5pm, the 72 hours still apply.

And the GDRP breach notification requires more than just saying you have had an incident. You'll have to include categories of data, records touched, and approximate number of data subjects affected. And this means you'll need some detailed intelligence on what the hackers and insiders were doing. Over the weekend. When your Head of IT is away fishing.

7. Fines

The GDPR has a tiered penalty structure that will take a large bite out of offender's funds - and the rules apply to both data controllers and processors. That means 'the cloud', so the huge cloud providers are not off the hook when it comes to GDPR enforcement.

Non-compliance results in fines of up to 4% of global revenue per incident.

This can include violations of basic principles related to data security - especially PbD principles. A company can be fined up to 2% of global revenue for not having their records in order, not notifying the supervising authority and data subjects about a breach or not conducting impact assessments.

SO WHAT NOW?

Companies through their key Data Officers or by outsourcing, which is permitted are responsible for creating access controls, reducing risk, ensuring compliance, responding to requests, reporting breaches within 72 hours and even creating a good data security policy.

AND, if you thought leaving the EU might get you off the hook, you can think again. GDPR will at least for the moment continue to apply as if we remain members of the EU.

So any UK companies that have part of their operations within the EU will have to continue abiding by this regulation.

YOU NEED TO TAKE ACTION!

The Security Circle can help you put together your plan for;

- **Data classification** - Know where personal data is stored on your system, especially in unstructured formats in documents, presentations, and spreadsheets. This is critical for both protecting the data and also following through on requests to correct and erase personal data.
- **Metadata** - With its requirements for limiting data retention, you'll need basic information on when the data was collected, why it was collected and its purpose. Personal data residing in IT systems should be periodically reviewed to see whether it needs to be saved for the future
- **Governance** - With data security by design companies should focus on data governance basics. For unstructured data, this should include understanding who is accessing personal data in the corporate file system, who should be authorised to access this data and limiting file permission based on employees' actual roles - i.e., role-based access controls. Process is going to be equally important and demonstrating compliance a key aspect GDPR Governance.
- **Monitoring** - The breach notification requirement places a new burden on companies data personnel. Under the GDPR, the IT security mantra should "always be monitoring". You'll need to spot unusual access patterns against files containing personal data and promptly report an exposure to the local data authority. Failure to do so can lead to enormous fines, particularly for multinationals with large global revenues.

To find out more about The Security Circle's GDPR Consultancy Services, please call Scott Simpson on:
0207 887 2618 *or email:*
GDPR@thesecuritycircle.com

LONDON
43 Berkeley Square, Mayfair, London W1J 5AP, UK
T: +44 (0)207 887 2618

GLASGOW
272 Bath Street, Glasgow, G2 4JR Scotland, UK
T: +44 (0)141 278 6422

DUBLIN
3 Park West Road, Park West, Dublin D12 DH93, Ireland
T: +353 1 453 3108

ZURICH
Churerstrasse 98, CH-8808 Pfäffikon/Schwyz, Switzerland
T: +41 (0)55 511 5100

www.thesecuritycircle.com