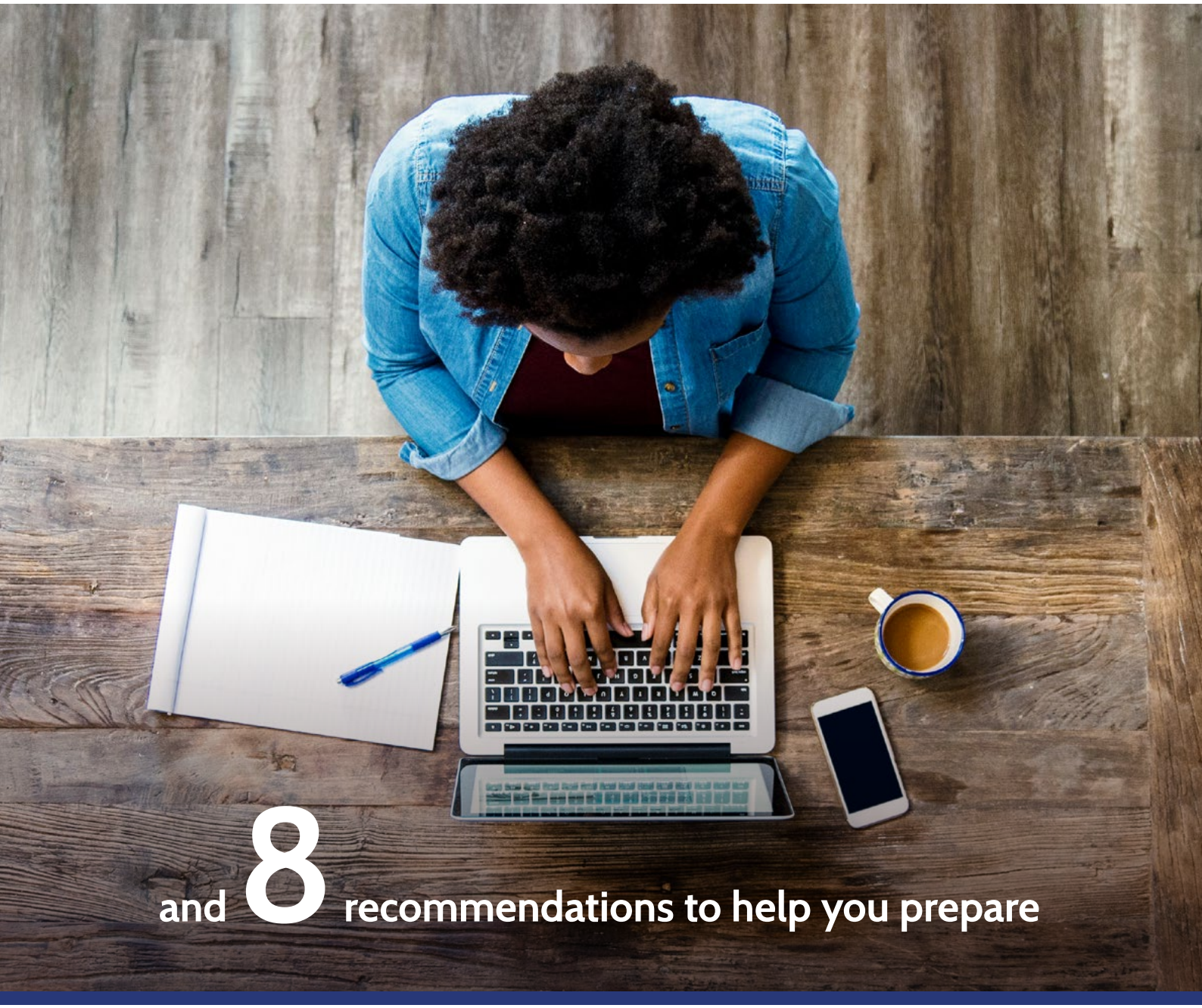
GDPR
in a nutshell

ST2
Technology.Connected



and 8 recommendations to help you prepare

By Richard Hannah

Managing Director of ST2 Technology, a Data Privacy Expert, former Data Privacy Lawyer and Global Transformation Director with 35 years of business experience.

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) will enter into force in May 2018. It will create a single law on data protection across the EU. It will have a significant impact on organisations in Europe as well as any organisation (wherever situated) that may hold data on Europeans. This data may be customers, business partners or employees.

Individual rights

If you simplify the rights to the individual that the GDPR introduces, it is simply this:

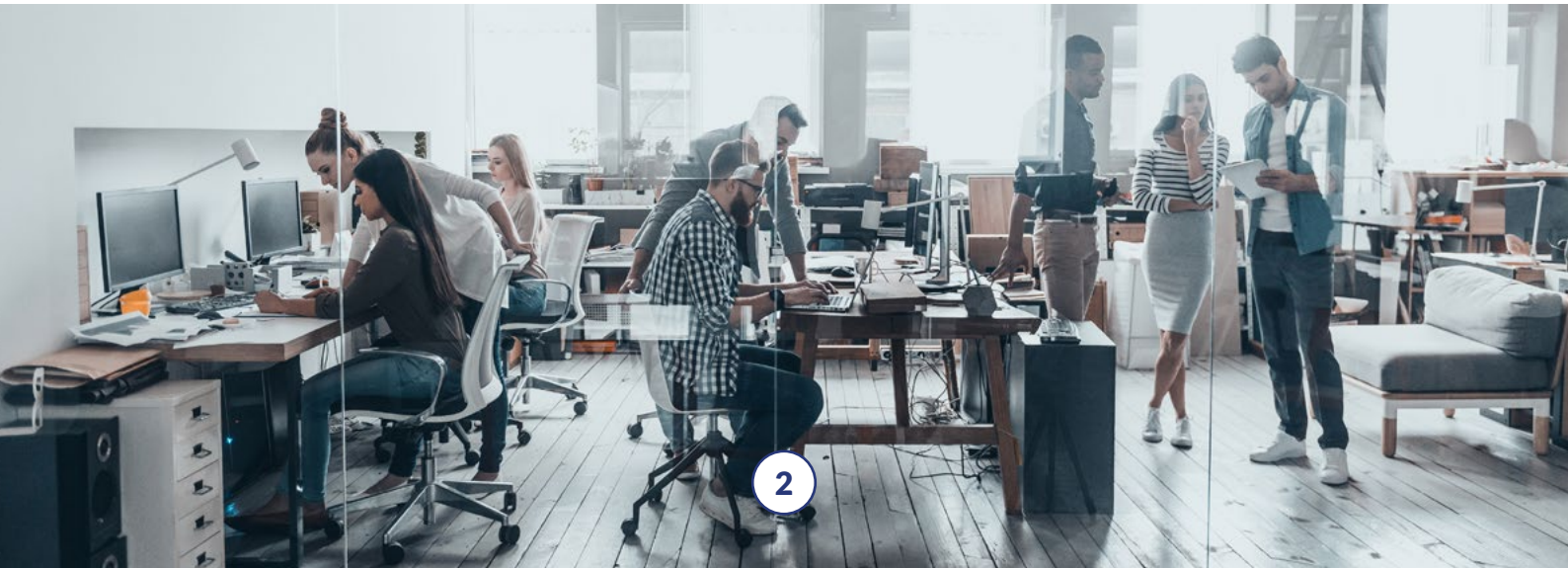
1. You must get consent to hold data on a person, and you must explain why you hold that data and for how long.
2. A person can ask you for information you hold on them and you are obliged to provide it. Information includes written and digital records.
3. A person has the right to demand that you remove their details from your records.
4. If you transfer data outside your borders it must be protected.

Compliance

All of this is eminently sensible, but requires investment for **all** organisations to comply. The challenge is that there are few exemptions other than the obvious - defence, police, NHS and (surprisingly) the media.

Organisations that hold data to meet their legal obligations (or to fulfill a statutory purpose) are **not exempt** from the Act. They simply do not have to comply with requests to **remove** details or **ask consent** to hold data. They must however comply with all other aspects of the GDPR.

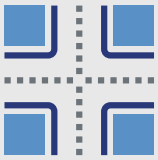
In the UK, the GDPR replaces the 20-year-old Data Protection Legislation. It introduces legislation with significantly more powers to punish non-compliance. The Regulator will have powers to impose significant fines for non-compliance of up to 4% of annual **worldwide** turnover for a corporate group. Non – commercial organisations will face fines, reputational damage and of course compensation claims from those impacted. It is anticipated that 'PPI' style agencies will switch from targeting PPI claims (which end in 2019) to claims for compensation under the new laws.



Impact

With only a few months to go until the GDPR becomes law, organisations should now seriously consider the impact of the GDPR by carrying out a comprehensive internal gap analysis of current data privacy and cybersecurity practices as compared to the GDPR requirements. The ICO provides free recommendations; we set out below some broad-brush recommendations as a starter:

8 recommendations to help you prepare



1. Data mapping

In English, that is to map and understand where your data is, what data is deemed sensitive and understand where your data comes from.

2. Scope

Garner an understanding of what the GDPR applies to (for instance):

- Any EU based controller (user) of personal data and anybody who processes data on their behalf. For instance, if you outsource your IT services or transfer information to associate businesses and organisations;
- An entity with no EU presence at all, which processes the personal data of an individual in the EU. That could be an outsourced business in India or China, for instance.

3. Data protection impact assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) should be completed when using new technologies and where processing techniques are likely to result in a high risk to individuals (e.g. employee monitoring). DPIAs need to be done now for **current** activities.

4. Content, notices and policies

Consent is king. Providing detailed privacy information to individuals will be required under the GDPR (such as how long data is retained). To be compliant, consent must be unambiguous and specific. Separate consent is required for each use of data. This will have significant impact on organisation such as charities, those who run membership schemes, local authorities and all of us who invest heavily in CRM systems. Data brokers will need to rethink their business models.

5. Individuals' new privacy rights

Understand the new privacy rights of individuals including rights to...

- Erasure of data (e.g. when data is no longer necessary or consent is withdrawn)
- Object to processing, including in relation to direct marketing
- Data portability (i.e. transferring data to another controller where processing is based on consent or on contract performance)

Organisations will need systems to provide proof. 'Yes, we did that' is not compliant.

6. Restrictions on profiling

The GDPR imposes new restrictions on organisations that conduct automated decision-making, e.g. profiling (essentially any form of analysis of personal data) with some exceptions.

7. Mandatory data breach reporting

Under the GDPR, personal data breaches must be reported without undue delay to the data protection authority and, where feasible, within 72 hours. Where the breach is likely to result in a high risk to affected individuals, they must also be notified without undue delay. Organisations should implement appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and loss/destruction of or damage to personal data.

8. Amending your contracts

Under the GDPR, we recommend your procurement contracts are reviewed and amended to contain obligations for your suppliers to:

1. Assist with data subjects' rights requests.
2. Notify you of data breaches.
3. Assist you with DPIAs.

If you supply a service or product, you may find your customers and business partners asking you to do the same thing.

Got any GDPR questions or issues? Arrange for one of our consultants to discuss what we can do to help you.

Contact us

+44 (0) 207 1834701

info@st2-technology.com

The GDPR is a hefty piece of legislation, don't ignore it! But see the act as an opportunity and not a red tape challenge. Beware of the GDPR know-all's who want to split the atom with their encyclopedic knowledge of the act; ultimately the ICO is taking a sensible line on the Act. Look to those who can support your implementation of the act operationally and pragmatically rather than those who wish to argue the toss about interpretation.

ST2 Technology.Connected