Topics

• Appreciating the value of policies and procedures
• Increased data incidents, data subject requests, regulatory investigations and fines
• Why GDPR is setting the tone for global privacy
GDPR Transparency and Accountability

ARE WE DONE YET?

GDPR implementation was just the start...

- GDPR laid the groundwork
- Legacy systems and people
- Anything else?

ARE WE DONE YET?

GDPR implementation was just the start…

- GDPR laid the groundwork
- Legacy systems and people
- Anything else?
Beyond GDPR: Data Governance is the ultimate prize!

- Data dictionary
- Data quality
- Centralised decision making and prioritisation
- Single customer view
- Issues and escalation
- Data retention and deletion decisions
- Capabilities are fit for compliance
- Exec level buy-in and accountability

Data Protection

**Data subjects rights**

- Automated decision making / profiling (Art 20)
- Access (Art 15)
- Object (Art 19)
- Rectification (Art 16)
- Data portability (Art 18)
- Erasure (right to be forgotten) (Art 17)
- Restriction of processing (Art 17a)
- Information (Art 14)
<table>
<thead>
<tr>
<th>Right to...</th>
<th>Necessary for contract</th>
<th>Legal requirement</th>
<th>Legitimate interests</th>
<th>Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Applies</td>
<td>Applies</td>
<td>Applies</td>
<td>Applies</td>
</tr>
<tr>
<td>Be informed</td>
<td>Applies</td>
<td>Applies</td>
<td>Applies</td>
<td>Applies</td>
</tr>
<tr>
<td>Rectification</td>
<td>Applies</td>
<td>Applies</td>
<td>Applies</td>
<td>Applies</td>
</tr>
<tr>
<td>Erasure¹</td>
<td>Applies if data no longer needed or processing is unlawful</td>
<td>Does not apply unless data no longer needed</td>
<td>Applies if individual has objected and there are no overriding legitimate grounds for processing</td>
<td>Applies unless no other legal basis for processing</td>
</tr>
<tr>
<td>Restrict processing</td>
<td>Applies if contesting accuracy or lawfulness or if individual needs to retain data</td>
<td>Applies if contesting accuracy or lawfulness or if individual needs to retain data</td>
<td>Applies if individual has objected to legitimate interests, or if contesting accuracy or lawfulness or if individual needs to retain data</td>
<td>Applies if contesting accuracy or lawfulness or if individual needs to retain data</td>
</tr>
<tr>
<td>Portability</td>
<td>Applies</td>
<td>Does not apply</td>
<td>Does not apply</td>
<td>Applies</td>
</tr>
<tr>
<td>Object to processing</td>
<td>Does not apply</td>
<td>Does not apply</td>
<td>Apply – assessment required</td>
<td>Does not apply*</td>
</tr>
<tr>
<td>Object to marketing</td>
<td>Applies</td>
<td>Applies</td>
<td>Applies</td>
<td>Applies</td>
</tr>
<tr>
<td>Automated decisions &amp; profiling</td>
<td>Does not apply</td>
<td>Does not apply</td>
<td>Applies</td>
<td>Does not apply*</td>
</tr>
</tbody>
</table>

*But consent may always be withdrawn

---

**Brexit campaigner AggregateIQ challenges UK’s first GDPR notice**

Canadian biz faces massive fine for allegedly exploiting personal info from Facebook

**Google hit with £44m GDPR fine over acts**

Chris Fox
Technology reporter
1 hour ago • Technology

Google has been fined 50 million euros (£44m) by the French data regulator CNIL, for a breach of the EU’s data protection rules.

CNIL said it had levied the record fine for “lack of transparency, inadequate information and lack of valid consent requiring swift execution measures”.

**Oi, you. Equifax. Cough up half a million quid for fumbling 15 million Brits’ personal info to hackers**

UK watchdog demands max penalty after security snafu

By Chris Williams, Enter in 2018 at 30 Sep 2018 at 13:13 • SHARE •
Sanctions for non-compliance are more than just for data breaches

Sanctions for non-compliance – two levels of fines…
➢ Up to the greater of 2% annual worldwide turnover of preceding financial year or EUR 10 million – for matters re internal record keeping, data processor contracts, data protection officers, data protection by design and default

➢ Up to the greater of 4% annual worldwide turnover of preceding financial year or EUR 20 million – for matters re breaching data protection principles, conditions for consent, data subjects’ rights and international data transfers

That dam breach or that damn breach?
Brexit: Deal or no deal

Deal or No Deal

Deal
- Transition period from 11pm GMT to 31 Dec 2020
- Most EU law will apply whilst details are worked out

No deal
- EU law stops applying at 11pm GMT
- UK cannot rely on reciprocity in Brussels Reg on jurisdiction and enforcement of judgments
- UK cannot rely on intra EU data transfers
- UK is out of the single market and customs union and no more mutual recognition of professional qualifications
Data Transfers pre Brexit

- Consent
- Codes of Conduct
- Contractual necessity
- Adequacy decision
- Privacy Shield
- BCR
- SCC

Brexit and data transfers

- Adequacy decision
- Negotiated arrangement
- Third country status
- SCC
- BCR
- ODTA
- Other grounds such as consent and legal necessity
Brexit and other data consequences

2013 Study on Trade Secrets

75% of respondents ranked them as strategically important to:
✓ Growth
✓ Competitiveness
✓ Innovation

Examples are:
➢ Commercial bids and contracts
➢ Contract terms
➢ Customer/supplier lists
➢ Financial data
➢ R&D data
➢ Process know how and technology
➢ Formulae and recipes
➢ Product technology
➢ Marketing data
Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure

- Harmonises the definition of trade secrets
- Provides civil law rights to stop unlawful use and further disclosure of misappropriated trade secrets
- Right to have products removed from the market that have created using illegally acquired trade secrets
- Right to compensation

❑ A trade secret must be seen by the business as secret

❑ It must be treated as secret by the business

How to protect trade secrets

✔ Clean desk policy
✔ Shredding
✔ Use of NDA's and Confidentiality Agreements
✔ Mark materials as CONFIDENTIAL
✔ Take care when emailing attachments
✔ Consider risks of disclosing trade secrets in public places
✔ Manage devices in the workplace
✔ Train staff to protect trade secrets
Often the biggest threat is ourselves

I changed all my passwords to "incorrect".

So whenever I forget, it will tell me "Your password is incorrect."
Trader boasted about secret deals on WhatsApp

A CITY investment banker has been fined more than £37,000 for boasting about deals on messaging service WhatsApp. Christopher Niehaus, 49, was a managing director at Jefferies when he bragged to pals about how he might pocket a bonus big enough to pay off his mortgage.

Investigators found conversations about deals – including one with a rival business – and the boasts. When confronted, Niehaus said he knew the information was confidential and should have known better. The FCA accepted that no one involved had traded any shares based on the inside knowledge and hit Niehaus – who, according to his LinkedIn profile, had previously worked at HSBC and Swiss lender UBS – with a £37,098 penalty.
The Rabbi Shmuley and Steve Bannon selfie. Credit: Twitter / @RabbiShmuley

Expanding Privacy Regulations
Understand your personal data estate

How do the laws apply

1. Think about history
2. Remember colonisation and conquest
3. Commonwealth countries adopt a UK approach, so Singapore, South Africa, Canada, India and Australia have English style laws
4. Spain and Portugal influence Argentina, Uruguay, Brazil and Macau
5. France influences North Africa, Vietnam and Canada
So in implementing policies and procedures…..

<table>
<thead>
<tr>
<th>EEA (GDPR)</th>
<th>EU influenced GDPR style</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law &amp; Regulation</td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>Rest of the world</td>
</tr>
</tbody>
</table>

Questions?
Thank you

Bristows LLP
100 Victoria Embankment
London EC4Y 0DH
T +44(0)20 7400 8000
robert.bond@bristows.com