A quick guide

to the new EU General Data Protection Regulation (EU GDPR)

Standard Life
There's a lot to look forward to

The definition of personal data is being extended from name, date of birth, gender etc to include:

- Biometric
- Genetic
- Mental Health
- Cultural
- Social Identity

Strengthened individual rights

Individuals have the right to request 'to be forgotten' (erasure of their personal data).

Individuals have the right to request a copy of their personal data in a portable format.

Individuals have the right to clear and transparent information; explaining what personal data we need; who this will be shared with and why; and that we will ensure its privacy.

Relying on consent to process personal data?

An individual's consent should be freely given and indicate an affirmative response. Silence is not valid consent.

Parental consent required for processing the personal data of their children.

Greater accountabilities for data controllers and obligations for data processors

Data Controller must ensure adequate provisions are documented in contracts to govern data processor (e.g. 3rd party suppliers). Data processors can now be held directly liable to the regulator for breaches of individuals' data.

Data Controller must notify regulator (UK Information Commissioner's Office) within 72 hours of a breach where there is likely to be a high risk of harm to individuals. Data Processors must notify the Data Controller of any breaches without undue delay.

An assessment of the impact on an individual's privacy was previous best practice and is now essential to understand any risk associated in processing their personal data.

Do the right thing.

OR

Tough new monetary penalties 4% of global turnover or €20 million (whichever is greater).

AND

Significant brand and reputational damage.

Are you ready – can you evidence this?

Standard Life
There's a lot to look forward to

Data Security and Breach Notification

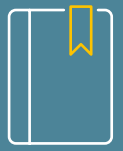
Need to be able to prevent, detect, and investigate breaches of your clients' data (and where there is a high risk of harm to your clients, you are able to notify the regulator within 72 hours of being aware of a breach).

Ensure any suppliers/third parties are able to notify you 'without undue delay' as soon as they are aware of a breach of your clients' data.

Fair Processing (Privacy) Notice

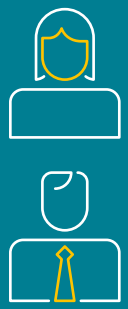
Privacy Notices to provide clear, concise information to your clients on what data is being processed, why you're processing it, who you are sharing it with (and why) and where their data is processed.

Explain what your clients' rights are and how to exercise them.



Strengthened individuals' rights

Your clients have the following rights:
'right to clear, concise information'
'right to request erasure of data'
'right to rectification of data'
'right of access to their data'
'right to restrict processing'
'right to data portability'
'right to object'



Accountability and Governance

Demonstrate ongoing compliance with data privacy obligations and ensure the privacy of your clients is considered [upfront] in all activities involving their personal data.

Suppliers/3rd parties

Document who processes your clients' personal data on your behalf. Review and amend existing contracts to include GDPR compliant clauses reflecting your respective obligations
Ensure you have assurance that their processes and controls are robust to keep your clients' data secure

Personal Data Inventory

Document what personal data is being processed, why, where and by whom (e.g. externally by suppliers/3rd parties).

Evidence to be documented that such processing is lawful under GDPR and meets regulatory principles for accuracy, retention etc.

Consent

If processing of personal data relies on your clients' consent, this must meet new GDPR standards to be valid. Needs to be freely given, specific and informed and an unambiguous affirmative action of their wish to 'opt in'
i.e. no pre ticked boxes,
silence is not consent.

1. Strengthened individuals' rights – do you have the processes and solutions in place to respond to requests from your clients when exercising their rights under GDPR?

2. Personal Data Inventory – can you evidence really what personal data is being processed, why and do your data management practices meet the minimum requirements?

3. Consent – have you got processes and solutions in place to capture and evidence clients' consent?

4. Suppliers/3rd parties – are you able to document who is processing your clients' data on your behalf, do you have a contract in place including GDPR clauses and have you checked their controls to ensure your clients' data is secure?

5. Fair Processing (Privacy) Notice – do your privacy notices provide clear, concise information to clients detailing how and why their personal data is processed and what their rights are?

6. Data security and breach notification – are your security controls robust to protect your clients' data? do you have a process for preventing, detecting, investigating and reporting a serious data breach to the regulator in less than 72 hours?

7. Accountability – remember, GDPR may have a deadline date of 25 May 2018 but do you have processes and controls in place to ensure you continue to meet your data privacy obligations beyond May?