Institute and Faculty of Actuaries

Managing Data – Understanding the Impact of the General Data Protection Regulation ("GDPR")

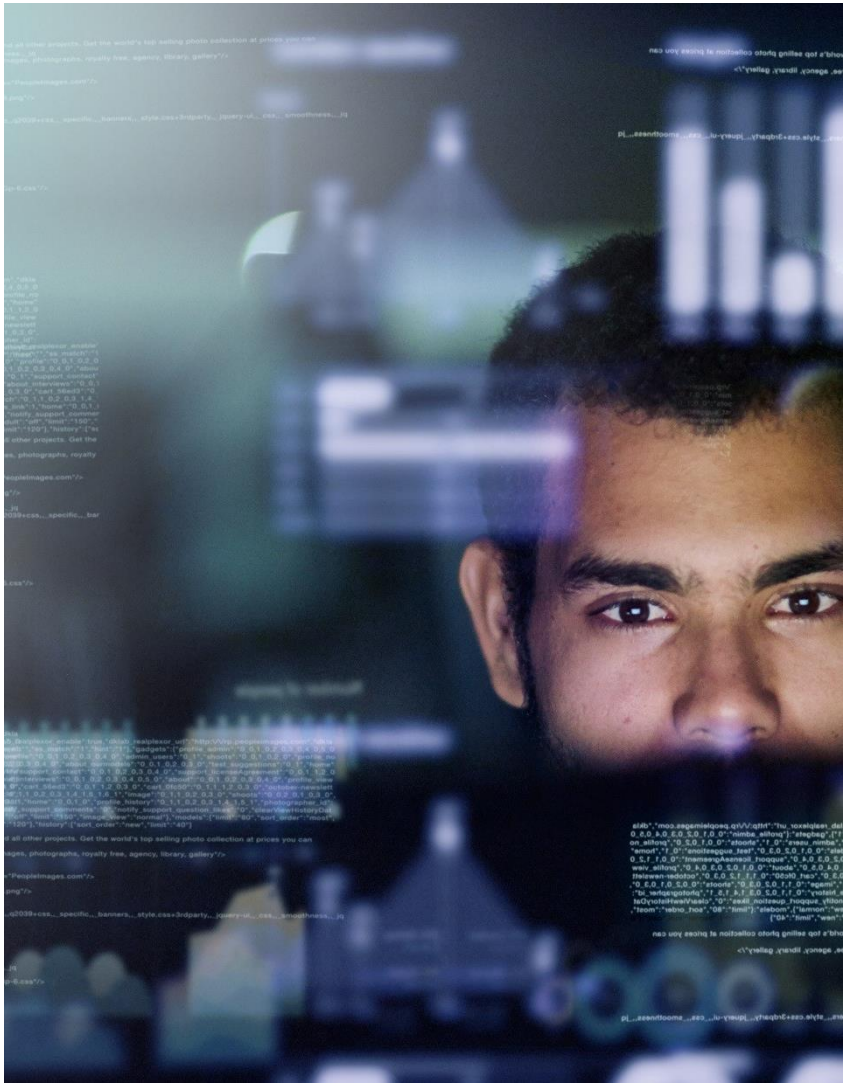
Ernst Landsberg EY
Shimon Simon EY

Institute and Faculty of Actuaries

Today's session

- Insights into the background of the regulation and the changes it is bringing.
- Practical lessons on recent engagements undertaken
- How data processing will be impacted and how to operate within the legal requirements.

Why do we need GDPR?

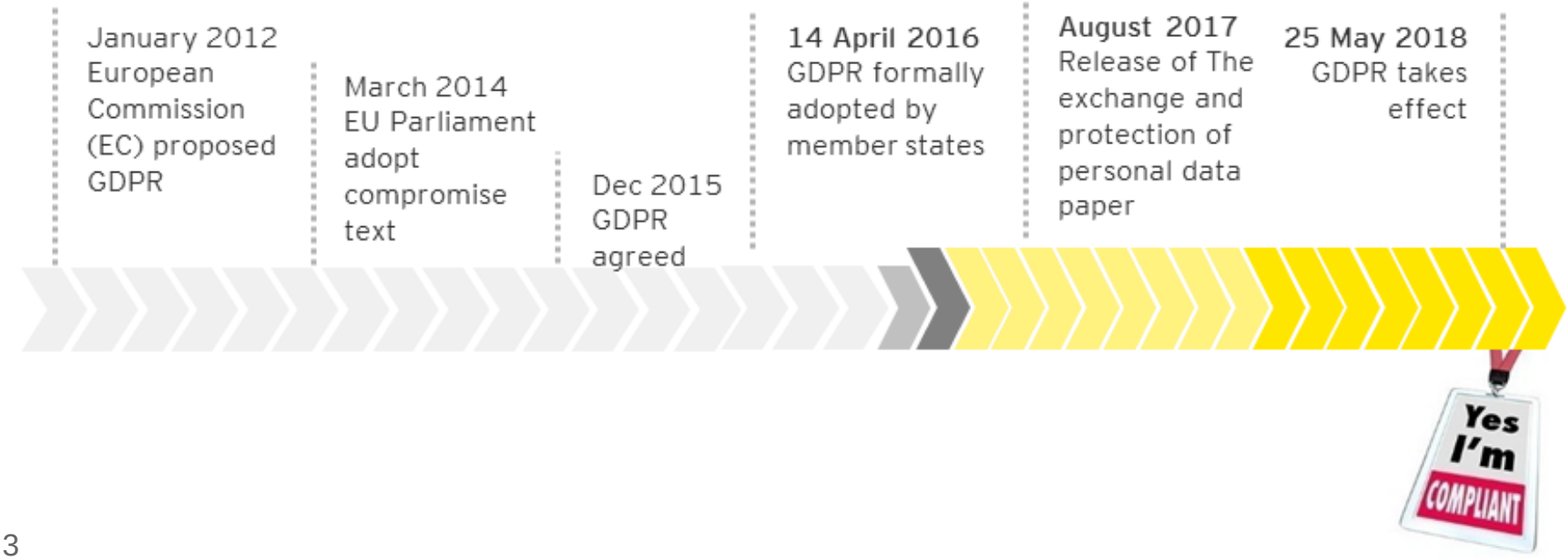


- ✓ Dispersed data protection regimes across the European Union
- ✓ Different standards applied by national regulatory authorities
- ✓ Technological developments form new types of threats for citizen's privacy
- ✓ Protect European citizen's privacy also outside of the European Union
- ✓ Facilitate data flow within the European Union

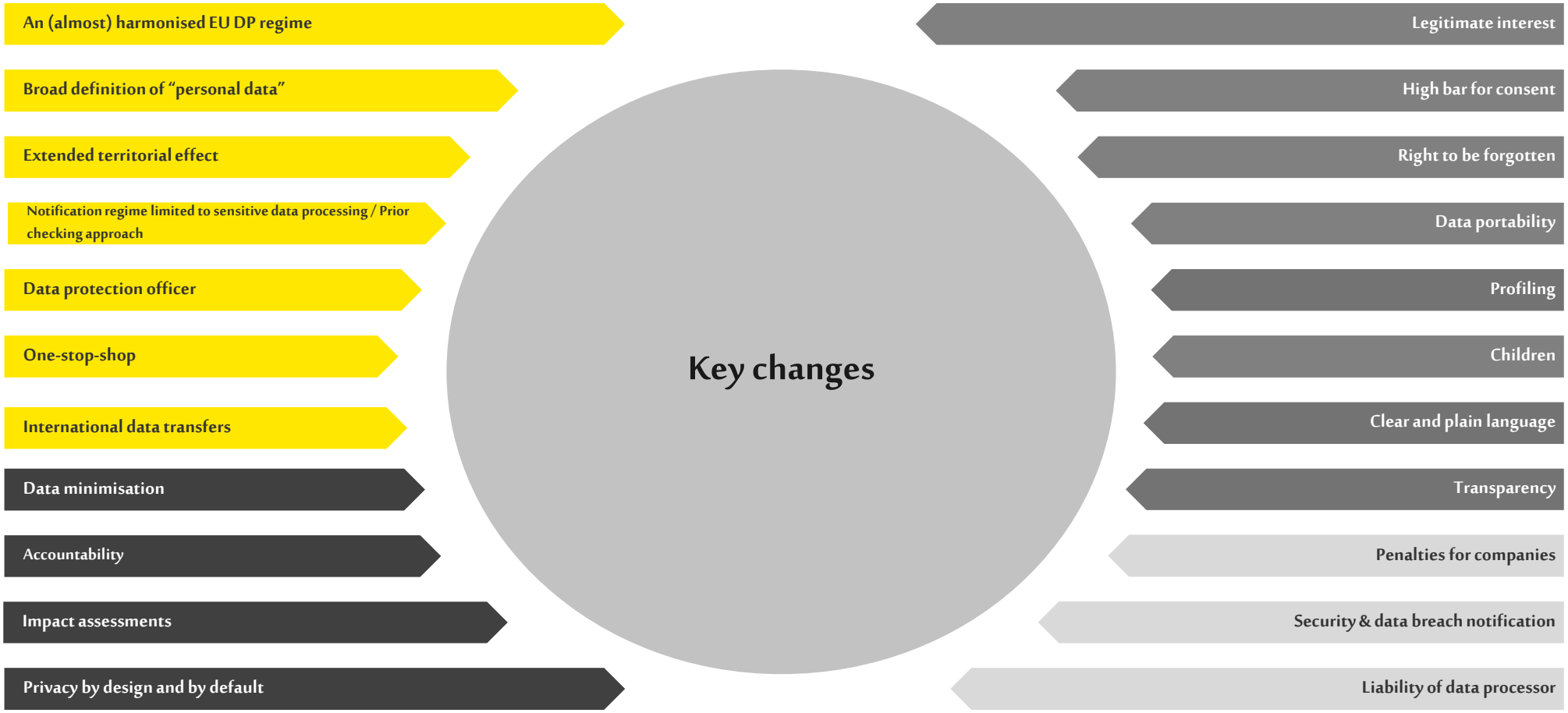
Why do we need GDPR?

- The volume of **people, process and technology change** required by the 25 May 2018 deadline of the GDPR should not be underestimated
- Many insurers are compliant, on paper, with existing legislation, but are yet to face the **challenge of implementing the requirements through the entire personal data lifecycle**
- As business models have been digitised, the **volume of data** held by organisations has increased significantly, resulting in organisations not **understanding how much PI they hold, why they retain it and how it is being used**

GDPR Timeline



GDPR insights – Key changes snapshot



GDPR key changes : Data Protection Principles

	Principle	Impact of Change
Fair, lawful and transparent processing	Personal data must be processed lawfully, fairly and ***in a transparent manner*** in relation to the data subject.	Enhanced compliance burden to document how processing is undertaken lawfully and fairly
The purpose limitation principle	Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. (Further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes, in accordance with Art.89(1),	Limited to no change for FS clients
Data minimisation	Personal data must be adequate, relevant and ***limited to what is necessary*** in relation to the purposes for which those data are processed.	Replaces “not excessive”. This more restrictive means firms need to carefully consider whether a processing activity is strictly necessary
Data accuracy	Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified ***without delay.***	Limited change as this was previously implicitly required. Failure to do so will though be a data principle breach incurring a the higher tier fine

GDPR key changes : Data Protection Principles

	Principle	Impact of Change
Data retention	Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific, historical, or statistical purposes in accordance with Art.89(1) and subject to the implementation of appropriate safeguards.	Limited to no change for FS clients.
Data security	Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	What was a previous Directive requirement is now a data protection principle. Information Security should now be seen as a fundamental obligation
Accountability	The controller is responsible for***, and must be able to demonstrate***, compliance with the Data Protection Principles.	Demonstrable compliance now required

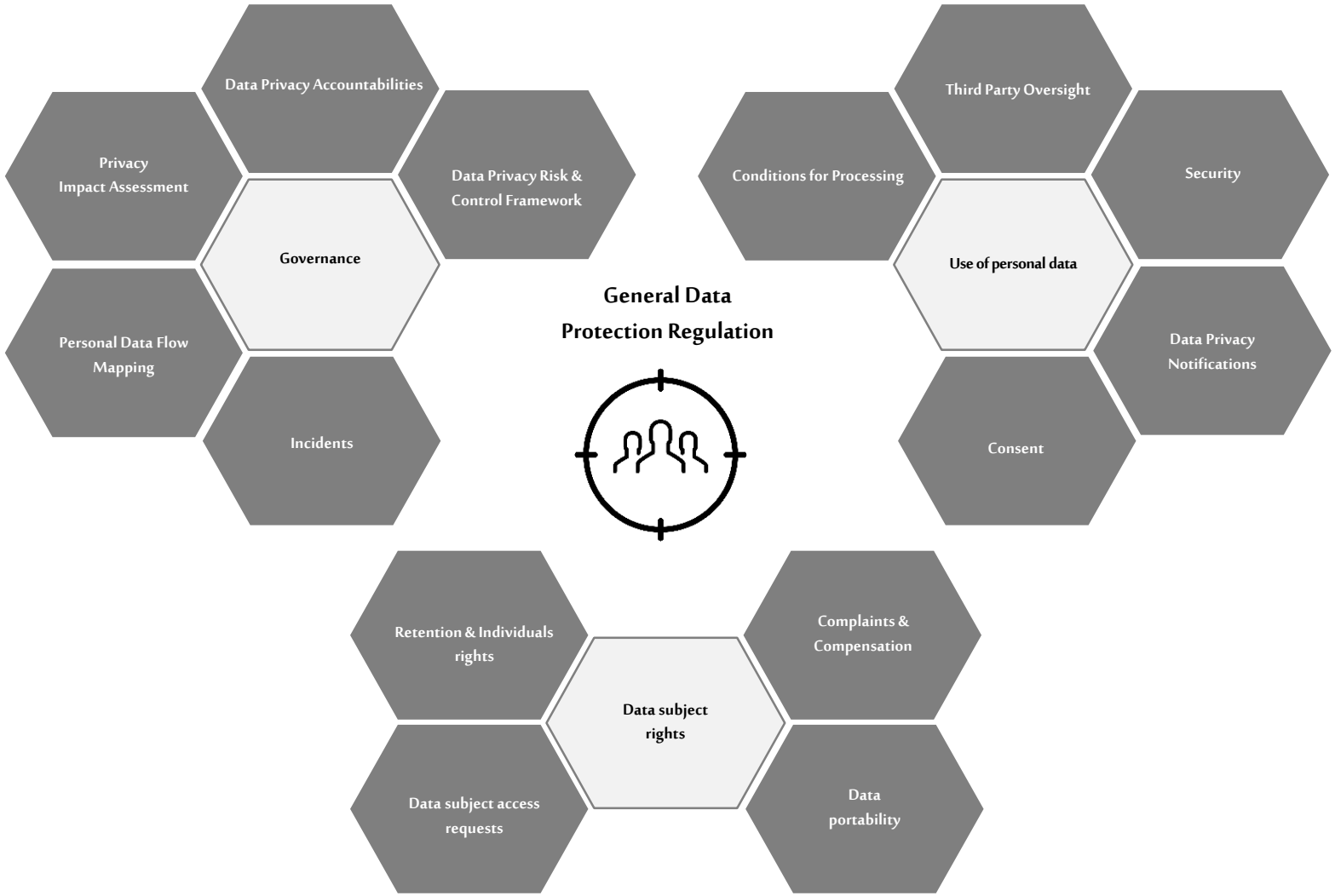
GDPR key changes (1/2)

Expanded scope	Applies to all data controllers and processors established in the EU and organizations that target EU citizens
Consent	▸ Consent must be provided by an and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"
New rights	▸ The right to be forgotten — the right to ask data controllers to erase all personal data without undue delay in certain circumstances ▸ The right to data portability — where individuals have provided personal data to a service provider, they can require the provider to 'port' the data to another provider, provided this is technically feasible ▸ The right to object to profiling — the right not to be subject to a decision based solely on automated processing
Privacy Impact Assessments	Organizations must undertake Privacy Impact Assessments when conducting risky or large scale processing of personal data
Privacy by Design	Organizations should design data protection into the development of business processes and new systems

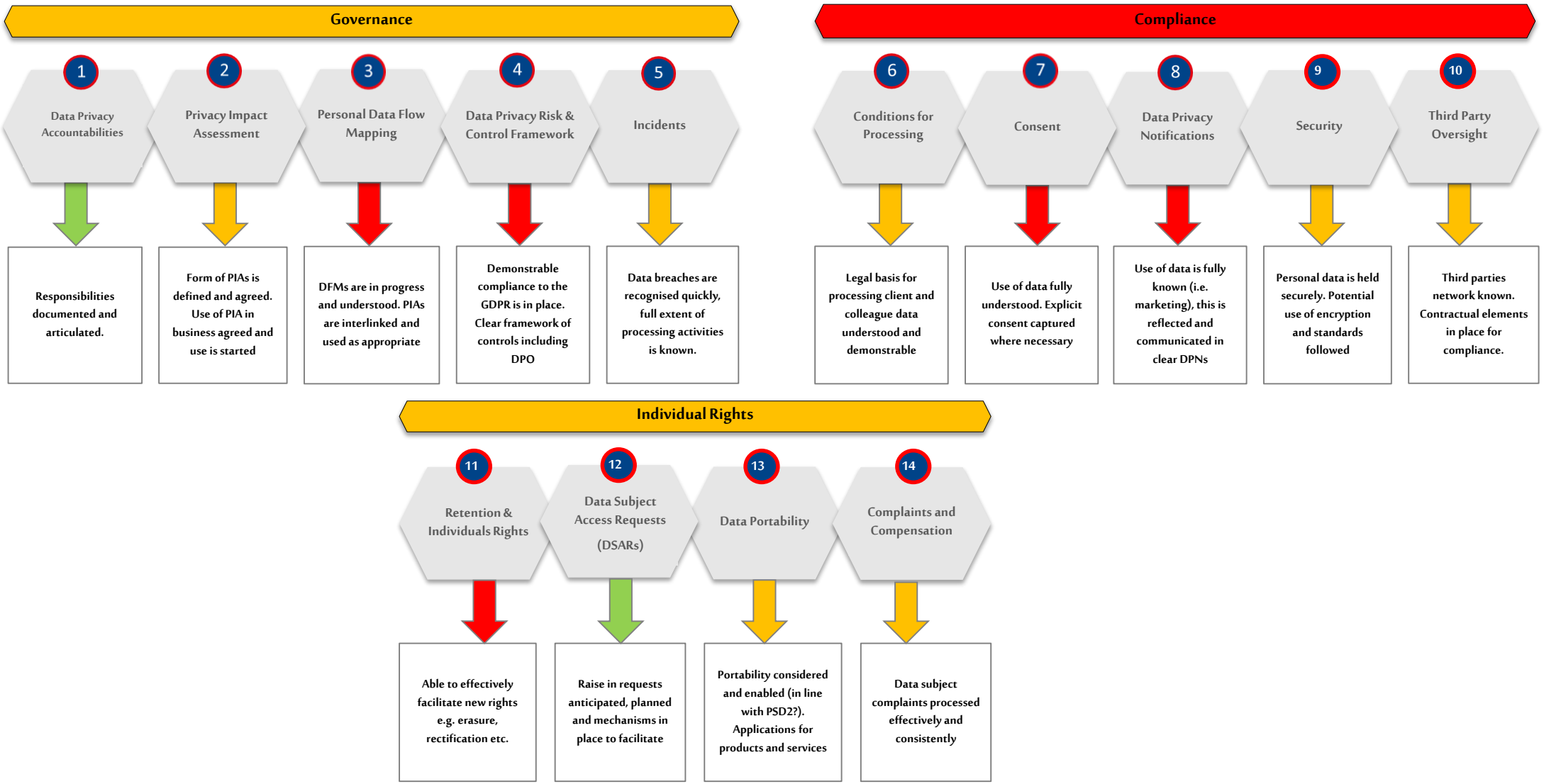
GDPR key changes (2/2)

Data Protection Officers (DPOs)	DPOs must be appointed if an organization conducts large scale systematic monitoring or processes large amounts of sensitive personal data
Accountability	Organization must prove they are accountable by: ► Establishing a culture of monitoring, reviewing and assessing data processing procedures ► Minimizing data processing and retention of data ► Building in safeguards to data processing activities ► Documenting data processing policies, procedures and operations that must be made available to the data protection supervisory authority on request
Obligations on processors	New obligations on data processors — processors become an officially regulated entity
Mandatory breach notification	► Organizations must notify supervisory authority of data breaches 'without undue delay' or within 72 hours, unless the breach is unlikely to be a risk to individuals ► If there is a high risk to individuals, those individuals must be informed as well
Fines of up to 4% of annual worldwide turnover	Fines for a breach of the GDPR are substantial. Regulators can impose fines of up to 4% of total annual worldwide turnover or €20,000,000, whichever is greater

GDPR: 14 Capabilities



GDPR: 14 Capabilities by Implementation Difficulty



Client challenges

Setting budget and resource allocation to GDPR programmes

Records of processing: Mapping through legacy IT systems and processes

Lack of industry consensus on approach to data portability

"Right to be forgotten" versus other regulatory and legal obligations

Linkage between the GDPR programmes and BAU activities

Dependency management – within programmes and within the business

Setting a clear vision and defining compliance for the organisation

Identifying the home for Data Protection and the new DPO role within the organisation

Data - the use of profiling within marketing activities customer profiling

Opt in vs. Opt out – historical and future approach to consent

Setting programme scope for GDPR and limiting scope creep

Manging communications and creating a 'culture of data protection'

Question & Answer – General

From a UK perspective, how different is GDPR from existing data protection requirements?

How is GDPR training being done is firms?

How are communications with customers changing as a result?

I keep hearing the expression "consent journey" - please can you explain what is meant by this?

What about policies that were incepted before more modern consent journeys?

What does "right to be forgotten really mean?"

Can we trust the Information Commissioner's Office (ICO) when it says that 100% compliance is not needed on May 2018 as long as material areas addressed, roadmap to full compliance laid out and resources allocated?

Surely the ICO will be gunning for Amazon and Google. Do they care about insurance companies?

What do you expect the ICO focus to be around insurance companies?

Question & Answer – Underwriting

Obviously for U/W purposes, Actuaries collect lots of personal data with consent - assume this is OK and they carry on? What about joint life cases?

An Actuarial valuation does not normally have a person's name, NI number, but sometimes you get detail on postcode, sex, DOB etc. and one could identify the person - is that a problem?

What about the Group policies - assume consent is required for all individuals?

What about process of health data and consent for use for GP reports?

We can start getting consent for new business, but what do we need to do about our existing customer base?

Question & Answer – Valuations

Clearly we can do experience analysis as before? But careful where extracts include personally identifiable data e.g. postcode, age, N.I.

Big issue is Actuaries like to store data on their own data stores and I assume this is a potential GDPR problem? What are the implications for them?

Life companies often use outsource providers - assume they will need to get p/h consent to share data with these firms?

Question & Answer – Transactions and buy-outs

Review how data shared between insurers and reinsurers will need consent or the data is anonymised?

Questions

Comments

Institute and Faculty of Actuaries