The GDPR – what is changing, and how will it affect you?

Chris Hudson - Proact IT Group AB General Counsel

PROACT

The GDPR – what is changing and how will it affect you?

Agenda

- What is it?
- How did we get here?
- Key provisions (why does it matter? / what is new?)
- What should we be doing now to prepare?

PROACT
Delivering Business Agility

What is it?

- The ‘General Data Protection Regulation’, (Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)

PROACT
Delivering Business Agility

What is it?

"on the protection of natural persons with regard to the processing of personal data and on the free movement of such data"

- Natural person = a real person, i.e. not a company or other legal entity
- Processing = any operation performed upon personal data whether or not by automated means (inc collecting, recording, organizing, structuring, storing, altering, retrieving, consulting, using, transmitting, disseminating, combining, erasing or destroying etc)
- Personal data = any information relating to an identified or identifiable natural person

PROACT
Delivering Business Agility

A quick history lesson

PROACT
delivering business agility

Development of EU Data Protection legislation

1953

ECHR – Article 8 Right
Respect for “private & family life”

1980

OECD guidelines on protection of personal data – 7 principles (Notice, Purpose, Consent, Security, Disclosure, Access, Accountability)

1995

Data Protection Directive adopted

2001

Implementation of the Directive in Member States

2012

Proposals for reform

2016

GDPR agreed

2018

GDPR comes into force

PROACT
Delivering Business Agility

Why was reform necessary?

- Significant technological advances over the years. (The ‘95 Directive was published before Windows 95 was released, 3 years before Google was founded,10 years before Facebook and Twitter. Quantities of data transmitted via Internet have multiplied by 42m times in the succeeding 20 years.)

- Variation of data protection law across the EU leading to inconsistencies and conflict and hindering free flow of data – old law based on Directive, new on ‘directly effective’ Regulation

PROACT
Delivering Business Agility

Why was reform necessary?

“17 years ago less than 1% of Europeans used the internet. Today, vast amounts of personal data are transferred and exchanged, across continents and around the globe in fractions of seconds. The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data. [These] proposals will help build trust in online services because people will be better informed about their rights and in more control of their information. The reform will accomplish this while making life easier and less costly for businesses. A strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation."

Vice President, EU Commission on launch of proposals - 2012

PROACT
Delivering Business Agility

Overview and key provisions of the GDPR

PROACT
delivering business agility

The reason you care – penalties!

- Maximum penalty for non-compliance is **4% of annual revenue or €20 million**, whichever is higher.
- Lower fines of up to 2% for administrative breaches, such as not carrying out impact assessments or notifying the authorities or individuals in the event of a data breach**.**
- Compare to current maximum fines under e.g. Latvian law (Personal Data Protection Law) – 14,000 EUR for administrative breaches, and 72,000 EUR max criminal fine.
- Puts data protection penalties into same category as anti-corruption or competition compliance.

PROACT
Delivering Business Agility

Scope

Applies to:

- Both data ‘controllers’ and to data ‘processors’.

  (Previously only affected controllers. Data processors now required to maintain records of personal data and processing activities, and to report breaches directly. Controllers now required to ensure contracts with processors comply with the GDPR.)

- Who ‘process’ EU citizens ‘personal data’. (Extra-territorial applicability)

  (Applies to processors based in EU, whether or not processing is in the EU. Also applies to processing of EU citizen’s data by a controller or processer established outside EU if offering goods/services to EU or profiling EU citizens. Non-EU businesses to appoint EU representative.)

PROACT
Delivering Business Agility

Basic principles

Article 5 of the GDPR – personal data should be:

- Processed lawfully, fairly and transparently
- Collected for explicitly specified and legitimate purposes and not further processed
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept no longer than necessary
- Protected with appropriate security (technical and organisational measures)

PROACT
Delivering Business Agility

Basic principles

Article 5.2 of the GDPR newly requires:

“the controller shall be responsible for and be able to demonstrate compliance with these principles”

This is the so-called accountability principle which now requires documented processes and evidence of compliance.

PROACT
Delivering Business Agility

Lawful processing

Main lawful bases for processing are:

- Consent
- Necessity
  - For performance of a contract
  - For compliance with a legal obligation
  - To protect the vital interests of the data subject or another person
  - For the performance of a task carried out in the public interest or the exercise of official authority
  - For the purposes of legitimate interests pursued by the controller or a third party except where overridden by the rights of the data subject.

PROACT
Delivering Business Agility

Lawful processing option 1 - consent

- Consent must be freely given, on an informed basis for a specific purpose and must be given unambiguously and verifiably
- Consent must consist of affirmative action. Silence, pre-ticked boxes (e.g on websites) or inactivity cannot constitute consent.
- Consent can be withdrawn at any time. New in the GDPR - it must be as easy to revoke consent as to give it. Opt in/out technical solutions may be the only viable option here.
- Data controllers and processors must be able to prove they had consent and the nature of it – so more detailed logs etc. are now a requirement.

Lawful processing option 2 - legitimate interest

- Not exhaustively defined, but examples include:

  for direct marketing, preventing fraud, transmission within a group of companies for internal admin, for ensuring information security or for reporting crime

- Controller must document its reasoning (impact assessments) showing it has considered the rights and freedoms of data subjects
- Must set out the specific operations it will perform to the subject in fair processing notices at the point at which data is collected
- New, the GDPR removes this ground for public authorities.

PROACT
Delivering Business Agility

Data subjects' rights

- To be informed (a fair processing notice, typically in a privacy policy etc)
- Access (new in the GDPR, subject access requests should be responded to without delay, within a month and without charge.)
- Rectification (inaccurate information must be rectified promptly and within a month, third party processors must also be told.)
- Erasure (right to be forgotten if consent withdrawn or object to processing and no overriding legitimate interest, or no longer necessary, third party processors must also be told.)

PROACT
Delivering Business Agility

Data subjects' rights - continued

- To restrict processing (controller must stop processing once an objection is raised relating to accuracy or legitimacy or where it is no longer needed or is unlawful but the subject requires the data to be retained – again and passed to third parties)
- To data portability (controller must provide data back in a structured commonly used machine readable format within one month – easy for e.g. CSV files, but how to supply video?)
- To object (where relying on legitimate grounds, must then demonstrate compelling grounds which override the freedoms of the individual – must tell of right to object when collecting data)
- In relation to automated decision making / profiling (right not to be subject to automated decision making without right for human input)

PROACT
Delivering Business Agility

Accountability and governance

Required to demonstrate compliance. Which means:

- Implementing technical and organisational measures that ensure and demonstrate you comply – i.e. data protection by design, e.g. by using technology, data classification, DP Impact Assessments
- Maintain documentation on processing activities
- In certain circumstances (public sector, systemtic/mass processors) appoint a DPO.

Evidence of compliance will be mitigation in a breach. The lower tier of fines can apply simply for failing to demonstrate compliance.

PROACT
Delivering Business Agility

Breach notifications

- Both controllers and processors liable in certain circumstances to report breaches to the relevant data protection regulator and in some cases to the individuals affected.
- A breach is any failure of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Notify supervisory authority if the breach results in a risk to the rights and freedoms of individuals
- Notify individuals if it is a ‘high’ risk – not clear what that means
- Notification must be made within 72 hours of becoming aware. 10m EUR or 2% global turnover fines for failure to do so. Obvious reputational damage flowing from disclosure.

PROACT
Delivering Business Agility

Data transfers

- GDPR maintains current position that transfers to “third countries” outside of EU is only permitted if they can demonstrate "equivalent" data protection laws. A small list of countries is ‘whitelisted’. Otherwise transfer is only allowed subject to binding corporate rules, model clauses or some other EU approved certification mechanism.

PROACT
Delivering Business Agility

Encryption and pseudonymisation

- Data held in an encrypted or pseudonymised form is not deemed to be personal data – falls outside the scope of the new rules altogether
- Warnings:
  - Data encrypted and considered secured using today's technology may become readable in the future
  - Risk of re-identification – Big Data analytics, who controls the keys?
  - Useful processing of that data may no longer be possible
- Consider format-preserving encryption/pseudonymisation – which renders anonymous but still allows selected processing of that data

PROACT
Delivering Business Agility

What should we be doing to prepare?

PROACT
delivering business agility

What should we be doing now to prepare?

- Audit your existing data flows for compliance – unlawful cross-border flows will trigger the highest penalties
- Prepare clear policies and procedures for dealing with breaches including notification
- Establish accountability framework – monitoring, reviewing, assessing data protection impacts
- Embed privacy by design into any new processing or product deployments
- Review/update privacy notices and policies on access requests and consider data portability/ formats
- Review your existing contracts with third parties who process on your behalf
- Consider technical solutions to compliance

PROACT
Delivering Business Agility

The GDPR - Summing up

- Biggest shake up of data protection legislation in over 20 years
- Increased penalties and notification requirements make the business risk significantly higher for non-compliance – this should be high on Board's agendas
- Increased territorial scope means everyone doing business in the EU will need to comply
- Privacy by design is now a legal requirement
- Data portability is now a legal requirement
- It is a legal requirement to implement sufficient technical security measures to secure personal data

PROACT
Delivering Business Agility

Questions?

PROACT
delivering business agility