Anderson Strathern

Anderson Strathern

The EU General Data Protection Regulation 2016 ("GDPR")

CodeClan

GDPR Awareness Training

20 April 2020

Douglas McLachlan
Partner, Anderson Strathern LLP
Head of Data & Technology

Key Points

Key Points

- GDPR came into force on 25 May 2018, replacing the Data Protection Act 1998
- Data Protection Act 2018 sits alongside and supplements GDPR
- Risk of substantial fines – (was previously only up to £500,000)
  - **€20 million** or **4%** of annual turnover, whichever is greater
  - **€10 million** or **2%** of annual turnover, whichever is greater
- Financial and reputational risks.
- Repackaged principles relating to processing personal data
- New accountability principle – makes things very process driven
- GDPR contains “processing conditions” that Controllers can rely on
- Importance of Privacy Notices, Terms & Conditions, Security Procedures, Policies etc

Anderson Strathern

Key Points

- Rights of data subjects (right to be forgotten; data portability)
- Data breach notification (72 hours)
- Data protection by design and default
- Focus on Data Protection Impact Assessments
- Data Protection Officers
- Role of data processors
- Tightening of Marketing rules – knowing the rules can help!
- GDPR continues to apply post Brexit!
- Data Analysts often process a lot of “Special Category” personal data
- Anonymised/pseudonymised data vs Personal Data
- Importance of GDPR Compliance & Data Ethics in designing data gathering/analysis exercises
- Controls on sending Personal Data outside the EEA

Anderson Strathern

GDPR Principles and Processing Conditions

Basic concepts

- **Personal Data** = "data" relating to a Data Subject (sometimes this is called "PII")
- **Data Subject** = an identified or identifiable natural person i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as:
  - a name
  - an identification number
  - location data
  - an online identifier
  - or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- **Pure statistical data** is not Personal Data
- **Anonymised data** is not Personal Data.
- **Pseudomymised data** remains Personal Data in someone's hands – i.e. the person who retains the "key". The data is not necessarily fully anonymised. It is a security feature.

Anderson Strathern

Basic concepts

- **Controller** = the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

- **Processor** = a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller

Anderson Strathern

Principles (Ch. II Article 5)

1. Lawfulness, fairness and transparency
   - (Detailed Privacy Notices have become very important)
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
   - **Accountability** – the controller shall be responsible for, and be able to demonstrate compliance with the above 6 principles. This makes things very process driven.

Anderson Strathern

Conditions for lawful processing

a. Data subject has given **consent** to the processing of his or her personal data for one or more specific purposes.

b. Processing **necessary for performance** of a contract to which **data subject** is a party or in order to take steps at the request of the data subject prior to entering into a contract

c. Processing is **necessary for compliance with a legal obligation** to which the controller is subject

d. Processing is necessary in order to protect **vital interests** of the data subject or another natural person

Anderson Strathern

GDPR - Conditions for lawful processing (cont.)

e. Processing is **necessary for performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller

f. Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where data subject is a child.

- **Often legitimate interests is a useful "catch all" condition that many businesses can use. You may use it for Marketing, for example.**
- **Note the balancing act here.**
- **May apply to a lot of data analysis and statistical processing of Personal Data.**
- **Remember, pure statistical analysis of fully anonymized data is not regulated by the GDPR.**

Processing of special categories of personal data – more restrictive

"Special Categories" – Article 9(1) (formerly known as "sensitive personal data" under DPA 98)

- Racial or ethnic origin
- Political opinions
- Religious of philosophical beliefs
- Trade Union membership
- Genetic Data
- Biometric data for the purposes of uniquely identifying a natural person
- Health
- Sex life
- Sexual Orientation

Anderson Strathern

Processing of special categories of personal data

a. the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b. necessary for the purposes of carrying out **the obligations and exercising specific rights** of the controller or of the data subject in the field of **employment and social security and social protection law** in so far as it is authorised by Union or Member State law…

c. necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. carried out in the course of its **legitimate activities** with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without consent;

Processing of special categories of personal data

e. relates to personal data which are manifestly **made public** by the data subject;

f. necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;

g. necessary for reasons of **substantial public interest**, on the basis of EU or MS law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or MS law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to professional secrecy;

i. necessary for reasons of **public interest in the area of public health,** … e.g. Covid-19 tracking apps

j. necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A key one for Data Analysts

Anderson Strathern

Processing for different/new purposes

- There are processes and controls on using Personal Data that was gathered processed for "Purpose A" for a new "Purpose B". Compatibility must be assessed.
- This may be important to the exercises Data Analysts are often asked to do.
- Assessment of the link between Purpose A and Purpose B
- Context of collection is important e.g.
  - relationship between Controller and the Data Subject
  - expectations of privacy and confidentiality
  - incentives to exaggerate
- Nature of the Personal Data – e.g. is it Special Category data? Criminal convictions data?
- Consequences to the Data Subjects of the use of their Personal Data for Purpose B
- Safeguards -e.g. encryption or pseudonymisation
- This is where Privacy Notices and scopes of informed consents often come in

Anderson Strathern

Penalties

GDPR Penalties

- Substantial fines under GDPR
  - **€20 million** or **4%** of annual turnover, whichever is greater
  - **€10 million** or **2%** of annual turnover, whichever is greater
- Under the DPA 98 – the highest fine was previously only up to £500,000
- This does not mean that the ICO will suddenly start issuing fines in the £Millions.
- ICO will exercise discretion.
- BUT - step change in risk. Good data governance is essential

Anderson Strathern

Data Breaches & “Privacy by Design”

Data breaches – Art 33

- '**personal data breach**' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data transmitted, stored or otherwise processed.
- Notification to ICO:
  - without undue delay and **within 72 hours** after becoming aware of breach, unless **unlikely** to result in a **risk** to the rights and freedoms of natural persons. If later, need to give reasons.
  - Notification must include specific information
  - Must document breaches, the facts, effects and remedial action.
- Notification to data subject:
  - without undue delay if **likely** to result in a **high risk** to rights and freedoms of natural persons.
  - Describe in clear and plain language and provide certain information.
  - Don't need to notify in have implemented appropriate technical and organisation protection measures e.g. encryption.

Anderson Strathern

Data protection by design and default/“privacy by design”

What does this mean in practice?

- Consider at early stage when deciding what personal data you need and how you are going to process it.
- Ensure that you are processing only as necessary and that you have a lawful condition.
- Implement appropriate technical and organisation measures to safeguard personal data and keep under review.
- Have clear policies and procedures. Attend training (and demonstrate this).
- Build into work process planning, design and development.
- Carry out Privacy Impact Assessments where required.

Anderson Strathern

Marketing

Marketing communications

- **"Consent" condition for marketing communications**
  - High bar – freely given, specific, informed and unambiguous. A statement or a clear affirmative action is required.
  - Can't rely on silence or inactivity.
  - Can't bury the consent in Ts&Cs.
  - Can't use "pre-ticked" boxes.
  - Consent can be given orally – but you'll need to have a system to record it.
  - Good idea to get layered consents – to email, mail, telephone etc

- **"Legitimate interests" condition for marketing communications**
  - Recital 47 to GDPR specifically mentions direct marketing as a potential "legitimate interest"
  - You need to balance the legitimate interest of marketing to your business against the data subject's rights and freedoms
  - Postal marketing
  - Telephone marketing to individuals who haven't previously objected to you or aren't on the Telephone Preference Service.
  - Particular rules on emails – generally different rules for emailing people who work at companies/LLPs ("Corporate subscribers") than for individuals/sole traders ("individual subscribers")

Anderson Strathern

Marketing

- **Privacy & Electronic Communications Regulations ("PECR")**
  - protection against electronic communications spam – emails, automated calling, SMS
  - must have explicit consent to direct marketing to "individual subscribers"
  - use of "pre-ticked" boxes to gather consent to marketing communications will not be lawful.

- **BUT - "Soft" opt-ins will still be available:**
  - where there's an existing customer relationship i.e. where you've obtained a person's details in the course of a sale or negotiations for a sale of a product or service;
  - where the messages are only marketing similar products or services; and
  - where the person is given a simple opportunity to opt out of future messages (i.e. unsubscribe options)
  - clearly only the same entity that originally obtained the contact details can use this

- If you are marketing your services, it will be permissible to use the "legitimate interest" condition as you are typically going to be emailing people who work at a company or LLP.

- There may be quirks in the law for emailing sole traders though. These will be "individual subscribers" so technically you'd need consent or to use the "soft opt-in".

- Respect any requests to be taken off a mailing list

Anderson Strathern

General issues

Rights of Individuals

- Right of **access** (Art 15)
  - No fee
  - 1 month to respond
  - Concise, transparent, intelligible, easily accessible form, using clear and plain language.
- Right to be **informed** (fair processing) (Art 13 & 14) – Privacy Notices
- Right to **rectification** (Art 16)
- Right to **erasure/'to be forgotten'** (Art 17)
- Right to **restriction of processing** (Art 18),
- Right to **data portability** (Art 20) e.g. with Energy Company
- Right to **object** (Art 21)
- Right to **compensation** for material or non-material damage as a result of an infringement of the GDPR.(Art 82)

Anderson Strathern

Right to be informed (fair processing) and privacy notices

- The right of individuals to be informed means data controllers have an obligation to provide 'fair processing information', typically through a privacy or data protection notice.

- Fair processing requirements in GDPR are more prescriptive than in DPA 98. In summary, the information that you will need to provide is:

  - identity and contact details of the controller (and the data protection officer)

  - purpose of the processing and the legal basis for the processing (condition) and legitimate interests of the controller or third party, where applicable
  - any recipient or categories of recipients of the personal data
  - details of transfers to third country and safeguards
  - retention period or criteria used to determine the retention period
  - existence of each of data subject's rights
  - right to withdraw consent at any time, where relevant
  - right to lodge a complaint with the ICO
  - source of personal data and whether it came from publicly accessible source
  - whether provision of personal data is part of a statutory or contractual requirement
  - the existence of automated decision making, significance and consequences.

Anderson Strathern

Final “Top Tips”

Final "Top Tips"

- Privacy by design and good data governance are essential
- Fully anonymise data if you don't need Personal Data
- Question the provenance of any Datasets
- Consider whether what you're doing falls within the scope of what the Personal Data was originally collected for – "*just because you can doesn't mean you should*"
- Be careful of adverse consequences for Data Subjects arising from your analysis
- There are detailed controls on automated decision making – "computer says no". Beware algorithms that embed biases
- Be careful to respect and preserve the confidentiality of Personal Data (especially Special Category Data) and share it securely and in the framework of a Data Sharing Agreement
- GDPR is a legal framework to regulate good data analysis – not to stop it altogether

Anderson Strathern

Questions?

Douglas McLachlan, Partner
DD 0141 242 7952
E douglas.mclachlan@andersonstrathern.co.uk