GDPR

The General Data Protection Regulation

https://www.emineouk.com

Transfers of data

- Within Europe
  - Member states will already be subject to GDPR
    - Data controllers may only appoint data processors which provide sufficient guarantees to implement appropriate technical and organisational measures to ensure processing meets the requirements of the GDPR
    - Processors are required to process personal data in accordance with the controller's instruction
    - Data processor activities must be governed by a binding contract with regard to the controller
- 3rd countries
  - Only under certain conditions
    - Adequacy decision
      - Countries must demonstrate
        - The rule of law
        - Access to justice
        - Respect for human rights & freedoms
        - Relevant Legislation
      - List published in the official journal of the EU
        - Reviewed every four years
    - Binding Corporate Rules
      - Only suitable for inter-company or inter-group transfers
    - Standard clauses adopted by comission
    - Approved code of conducts / certification mechanisms
      - EU-US Privacy Shield
    - Contractual clauses between controller & Processor
      - Must be authorised by supervisory authority

Emineo

- PCI
- 27001 / 27002
- Cyber Essentials
- Auditing
- Compliance
- GDPR - Data Protection
- IT Strategy
- Penetration Testing
- Training
- GDPR Workshops
- High uptime networks
- Network Defence
- Firewalls & UTM
- Information Security
- Malware Protection Strategies
- Endpoint & Mobile Security
- Server & Network Hardening

Data Subject Rights

- 6 Principals
  - Right to fair processing
- Right to access
  - Data Subject Access Requests
    - "the controller must provide the data subject with a copy of the personal data undergoing processing"
      - data subjects can also request
        - the purpose of data processing
        - the categories of personal data stored
        - where data has been (or will be) disclosed to other countries
        - how long the data will be stored
        - info on the source of the data
        - whether any automated decision making process have been applied and the consequences
      - No charge to data subjects
      - Provide data within 30 days
- Right to rectification
  - Process for data subjects to make changes
- Right to be forgotten
  - Right to erasure
  - Right to be forgotten
- Right to data portability
  - Right to a copy of their data
    - only when based on consent or contract;
    - and when processing is automated;
    - and when provided to the controller by the data subject themselves
  - "in a structured, commonly used and machine readable format"
- Right to object
  - Right to object to a supervisory authority

Personal Data

- Special Categories
  - subject to tighter restrictions and higher penalties for misuse
    - Racial or ethnic origin
    - Political opinions
    - Religious or philosophical beliefs
    - Trade union membership
    - Data concerning health
    - Sex life and sexual orientation
    - Genetic data
    - Biometric data
    - UK Addition
      - Criminal convictions
  - Processing prohibited unless specific lawful reasons
- Very broad definition of personal data
  - any information
    - Letters / Emails
    - name
    - Address
    - email address
    - IP address
  - realting to
    - an identified or identifiable
      - anonymous data is excluded
      - nautral person
        - does not apply to deceased people
        - does not apply to organisatioal data

Processors vs Controllers

- Each organisation may be a controller or processor for different sets of data
- Controller
  - "determines the purposes and means of the processing of personal data"
  - must store formal records
    - Of controller
    - Name and contact details
    - Purpose of processing
    - Description of the categories of data
    - Categories of recipients of data
    - Details of any international transfers of data
    - Time limits for erasure
    - Description of security measures
- Processor
  - "processes personal data on behalf of the controller"
  - must store formal records
    - Of processor and of controllers
    - Name and contact details
    - Categories of processing
    - Details of any international transfers of data
    - Description of security measures
- Joint Controller
  - "jointly determines the purposes and means of processing"
  - Same requirements as controller

Risk Assesments

- Data Privacy Impact Assessments (DPIA)
  - "processors and controllers should evaluate the risks inherent in the processing and implement measures to mitigate those risks"
  - Required when
    - When a systematic and extensive evaluation of personal data occurs on which decisions are based that produce legal effects or significant effects for the data subject
    - When processing, on a large scale, of special categories of data
    - When systematically monitoring a publicly accessible area on a large scale
  - Suggested under other circumstances
    - Need to consider any risk to the rights and freedoms of the data subjects. High risk data or high risk processes should trigger a DPIA

Breach Response Process

- What happened
- How did it happen
- What was breached
- What are the risk to data subjects
  - "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority"
    - Notify the authority
      - The nature of the personal data breach
      - name and contact details of the data protection officer
      - likely consequences of the personal data breach
      - measures taken or proposed to be taken by the controller to address the personal data breach
    - Notify within 72 hours
  - "the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons"
    - Also notify the data subjects
      - In plain and clear language
  - "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons"
    - No need to notify
- A breach response process need to be in place before a breach to ensure this happens in a timely manner.

6 Principles

- Lawful Basis
  - "Processing shall be lawful only if and to the extent that at least one of the following applies"
    - Personal Data
      - Consent
        - Given freely
        - Specific
        - Informed
        - Unambiguous
        - Able to be withdrawn just as easily
          - If relying on consent - it can be withdrawn at any time
          - Try to avoid consent if processing relies on any other lawful basis
      - Contract
        - Employment Contract
        - Sales Contract
      - Legal Requirement
        - HR / Tax Law
      - Vital Interest
        - Medical records
      - Public Interest
        - Police records
      - Legitimate Interest
        - Balance organisation interests against rights and freedoms of data subject
    - Special Categories
      - Explicit Consent
        - Must be opt-in
      - Employment, Social Security & Social Protection Law
        - e.g. HR - Must still be necessary
      - Vital Interests & Incapacitated
        - Must try to seek consent
      - Political, philosophical or religious non-profit
        - Exemption for churches ect
      - Defence of legal claims
        - Courts
      - Data is manifestly made public by data subject
        - For example twitter
      - Substantial public interest
        - Public Health
        - Scientific or historical research
      - Preventive or occupational medicine - medical & social care
        - Nurses, Doctors & Social Care
        - At the time the data is obtained
- Lawfulness, fairness and transparency
- Transparent & Fair
  - "... the data subject [should] be informed of the existence of the processing operation and it's purpose"
    - Have a clear privacy policy
    - Identity and contact details of the controller
    - Purpose of the processing and the legal basis
      - Lawful Basis
    - Categories of personal data
    - 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
    - Whether the provision of personal data part of a statutory or contractual requirement
    - The existence of automated decision making, including profiling
    - Details of data subjects rights
- Purpose limitations
  - "Personal data can only be collected for specific, explicit and legitimate purposes"
    - Don't change your use of data
    - Specific
      - Only collect for a specific purpose
    - Explicit
      - Can't change the use after collection
    - Legitimate
      - Ensure you have a lawful basis for that purpose
- Data minimisation
  - "Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"
    - If you don't need it - don't store it
    - Adequate
      - Collect enough to do the processing
    - Relevant
      - Only collect what is relevant to the processing
    - Limited
      - Don't collect things 'just-in-case'
- Accuracy
  - "Accurate and where necessary kept up to date"
    - Use appropriate information systems
    - Accurate
      - Systems should ensure accuracy
    - Up to date
      - Ensure data subjects can request changes
- Storage limitations
  - "Kept in a form which permits identification of data subjects for no longer than necessary"
    - If you don't know what you are storing - you can't guarantee it's still needed
    - Categorise Data
    - Check statue of limitations
      - Member state law requires certain retention of records
    - Ensure data is remove when no longer needed
      - Consider archives and backups
- Integrity and confidentiality
  - "appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage"
    - Consider the CIA Triad
      - Confidentiality
        - Ensure data is only shared with those authorised to process it
      - Integrity
        - Ensure data is not accidentally or maliciously modified
      - Availability
        - Ensure data is available when needed and protected from disasters
    - Consider an IT governance framework
      - ISO27001 / ISO27002
      - Cyber-Essentials
      - IASME Certification

Data Protection Officer

- Mandatory under certain circumstances
  - The processing is carried out by a public authority
  - core activities consist of processing operations requiring regular and systematic monitoring of data subjects on a large scale
  - core activities consist of processing special categories of data on a large scale
    - Key terms are 'core activities' and 'large scale'
      - core activities
        - Those things that are fundamental to the business model of the controller or processor. Not ancilliary functions such as HR.
      - large scale
        - Not explicitly defined. May refer to extent, duration, reach and volume.
- DPO Qualities
  - Professional privacy qualifications
    - Industry Qualifications
      - CIPP/E - Certified Information Privacy Professional/Europe - iapp
        - Certified Information Privacy Professional
  - Excellent understanding of privacy law
  - Experience implementing data protection measures
    - Industry Qualifications
      - CIPM - Certified Information Privacy Manager - iapp
        - Certified Information Privacy Manager
  - Experience managing key systems
  - Experience with risk management systems
  - Experience with information security management
    - Industry Qualifications
      - CISSP - Certified Information Systems Security Professional
        - Certified Information Systems Security Professional
- The DPO is a protected and independant role
  - "The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor."
    - Ensure the DPO is trusted
    - Ensure the DPO knows their field
    - Ensure the DPO is given appropriate access & resources
- DPO Duties
  - to inform and advise the controller or the processor
  - to monitor compliance with the GDPR
  - to cooperate with the supervisory authority and act as a contact point
  - to act as a point of contact for data subjects
- A DPO can be an internal employee or external consultant. Full time or part-time.

Emineo

A Geek-Guru Brand

Version 1.3 - Subject to change without notice. Please check website for latest version: http://bit.ly/2EL8hRq

Emineo GDPR Mind-Map

Copyright 2017 © Emineo™ Technology (Geek-Guru Ltd)

This document may be updated or changed without notice at any time. Use of the information is therefore at your own risk. In no event shall Emineo or Geek-Guru be liable for special, indirect, incidental or consequential damages resulting from or related to the use of this document.

The contents of this document are provided "AS IS". This information could contain technical inaccuracies, typographical errors and out-of-date information.