Naushad'S Msc Assignment Gdpr Audit Checklist

Other processor obligations

- Contracts with controllers
  - Are there controller/processor contracts in place containing the stipulated terms?
  - Is there written authorisation for existing sub-processing arrangements?
  - Use of sub-processors
    - Is there written authorisation for proposed sub-processing?
    - Has specific or general authorisation been provided?
    - If general authorisation, is there a process for informing the controller of any intended changes to processors?
    - Is the processing subject to a contract including stipulated terms?
    - Have the same obligations set out in the contract with the controller been imposed on the sub-processor?
  - Demonstrating compliance (record keeping)
    - How many employees does the company have?
    - Is sensitive personal data processed?
    - Are the legal grounds for processing personal data recorded?
  - Data Protection Officer (DPO)
    - Do you need to appoint a DPO?
    - If a DPO is not required, consider whether one should be appointed.
    - Where a DPO is appointed are escalation and reporting lines in place?
  - Assistance to data controller
    - Are you able to assist the data controller in ensuring compliance under the GDPR?

Other controller obligations

- Technical and organisational measures
  - What privacy training programmes does the data controller provide for employees?
  - Are there clear documented policies and procedures for all aspects of GDPR compliance?
  - Do you operate a regular audit review process?
- Privacy by design and default
  - Do policies and procedures build in a requirement to integrate compliance into processing activities?
- Data Protection Officers (DPOs)
  - Do you need to appoint a DPO?
  - If a DPO is not required, consider whether one should be appointed.
  - Where a DPO is appointed are escalation and reporting lines in place?
- Demonstrating compliance (record keeping)
  - How many employees does the company have?
  - Is sensitive personal data processed?
  - Are the legal grounds for processing personal data recorded?
- Data Protection Impact Assessments (DPIAs)
  - Do you have a process for identifying the need for and conducting (and documenting) DPIAs?
  - Do you undertake and record prior diligence of service providers?
- Data processor contracts
  - Are all the stipulated terms included in processor contracts?
  - Are there controller/processor contracts containing all the stipulated terms?

International data transfers (outside EEA)

- International data flow mapping
  - Is personal data transferred outside the EEA?
  - What type of personal data is transferred and does this include any sensitive personal data?
  - What is the purpose(s) of the transfer?
  - Who is the transfer to?
  - Are all transfers listed - including answers to the previous questions (e.g. the nature of the data, the purpose of the processing, from which country the data is exported and which country receives the data and who the recipient of the transfer is?)
  - Is the legal transfer adequacy mechanism for each transfer identified and listed?
- Legality of international transfers
  - Are specific transfers appropriately covered by an implemented adequacy mechanism or covered by an exception?
- Transparency
  - Are data subjects told of any intended transfers of their personal data?
- Transfers requested by overseas authorities or courts
  - Is there a policy for handling requests for disclosure/transfer of personal data to overseas authorities or courts? (The UK has opted out of this provision).

Data breaches

- Breach response obligations
  - Does the organisation have a documented privacy and security Incident Response Plan and incident identification systems?
  - Are the plan and procedures regularly reviewed and road tested?
  - Are there procedures in place to notify DPAs and data subjects of a data breach (where applicable)?
  - Is there clear internal guidance explaining when notification is required and what information needs to be reported?
  - Are there clear procedures in place to notify the controller in the prescribed form of any data breach without undue delay after becoming aware of it?
  - Are data breaches documented?
  - Are there cooperation procedures in place between controllers, suppliers and other partners to deal with data breaches?
  - Have you considered data breach insurance cover? (not mandatory under GDPR)

Data security

- Appropriate technical and organisational security measures
  - Are the risks inherent in the processing formally evaluated, tested and assessed and have measures to mitigate those risks and ensure the security of the processing been implemented?
  - Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data?
  - Is there a documented process for resolving security related complaints and issues?
  - Is there a designated individual who is responsible for driving remediation plans for security gaps?
  - Are industry standard encryption algorithms and technologies employed for transferring, storing, and receiving individuals' sensitive personal information?
  - Is personal information systematically destroyed, erased, or anonymised when it is no longer legally required to be retained or to fulfil the purpose(s) for which it was collected?
  - Are steps taken to pseudonymise personal data where possible?
  - Can the availability and access to personal data be restored in a timely manner in the event of a physical or technical incident?

Data subject rights

- Access to personal data
  - Is there a documented policy/procedure for handling subject access requests (SARs)?
  - Are individuals provided with a mechanism to request access to information held about them?
  - Is the data controller able to respond to SARs within one month?
- Data portability
  - Can data subjects get their personal data in a structured, commonly used and machine readable format?
- Erasure and rectification
  - Are individuals informed of their right to demand erasure or rectification of personal information held about them (where applicable)?
  - Are there controls and formal procedures in place to allow personal data to be erased or blocked?
  - Can lists and procedures manage such requests?
- Right to object
  - Are individuals told about their right to object to certain types of processing?
  - Are there policies to ensure rights can be effected in practice?
- Profiling and automated processing
  - Is profiling based on consent? (if so it has must be explicit).
  - Does any profiling use sensitive data?
  - Does any profiling involve children's data?

Other data protection principles and accountability

- Purpose limitation
  - Is personal data only used for the purposes for which it was originally collected?
- Data minimisation
  - Is the personal data limited to what is necessary for the purposes for which it is processed?
- Accuracy
  - Are policies and training in place to ensure personal data are checked and where inaccurate are rectified without delay?
- Storage limitation (retention)
  - Do privacy policies incorporate information on retention? Are there procedures in place for archiving and destruction of data?
- Integrity and confidentiality
  - Are appropriate security measures used to protect the data?
- Accountability
  - Can you demonstrate compliance with the data protection principles?

Transparency requirements

- Transparency requirements
  - Is the data subject notified of processing?
- Source of personal data and information provided to data subject
  - Is data collected direct from the subject and is the required information given to them?
  - Is the data not collected from the subject and is the required information given to them?

Personal Info

- Are you processing personal data?
  - Personal data
  - Sensitive (special) personal data
  - Children's personal data
- Is personal data of children collected and processed?

Scope of application

- EU controller
  - Are you a controller?
- EU processor
  - Are you a processor?
- Main establishment
  - Where is the main EU HQ?
- Non-EU controller / processor
  - Are any group companies located outside the EU that target/monitor EU subjects?
  - If so, has an EU representative established in one of the EU States where the data subjects are, been designated in writing (where appropriate)?
  - Is the EU representative mandated to be addressed (in addition to the controller / processor) by supervisory authorities and data subjects on processing issues?
- Joint controllers
  - Are there any joint data controller relationships?

Lawful grounds for processing

- Lawful grounds for processing
  - Is there a lawful ground for processing the personal data for each processing operation?
  - Is there a lawful ground for processing any sensitive personal data for each provessing operation?
- Consent
  - How is consent collected?
  - How is this consent demonstrated?
  - Can subjects withdraw their consent?

GDPR Checklist

By www.naushad.co.uk