GDPR Planning Checklist

Are you ready to get started in evaluating and implementing measures to ensure GDPR compliance? Complete our checklist below to get closer to the GDPR finish line. We hope that this is a great start in your race to GDPR compliance!

Identify the personal data fields that you are collecting from EU citizens.

- [ ] What personal data is collected and/or processed?
- [ ] Where is it stored or transmitted? For how long?
- [ ] What retention policies or processes apply to this data? Can this be reduced?
- [ ] Is it under your control or that of a contractor?
- [ ] Does this data remain in the EU at all times?

Characterise the consent information and processes that exist when collecting this data.

- [ ] Are data subjects asked in clear language for explicit consent to collect and process their data?
- [ ] Is consent granted at the time of collection?
- [ ] Does the consent communication identify and provide contact information to the controller, processor and Data Protection Officer (DPO) where appropriate?
- [ ] Does it describe the purpose of processing, security of processing, and legal basis?
- [ ] Does it provide the period for which the data will be stored?
- [ ] Does it name the recipients or category of recipients of the data?
- [ ] Does it explain the data subjects' rights to access, rectify, request erasure or make portable their data, as well as their right to complain to a supervisory authority?
- [ ] Does it state the intent to transfer the data outside of the EU?
- [ ] Does it stipulate whether data collection is mandatory or optional, as well as the consequences of not providing said data?
- [ ] Is it just as easy to withdraw consent as provide consent?

Characterise the ability to communicate with data subjects.

- [ ] How do data subject's access, rectify, have erased, and extract their data for transfer?
- [ ] How do data subjects withdraw consent?
- [ ] How does the organisation contact data subjects to report a breach?

Determine if current record-keeping measures and data processing policies are adequate.

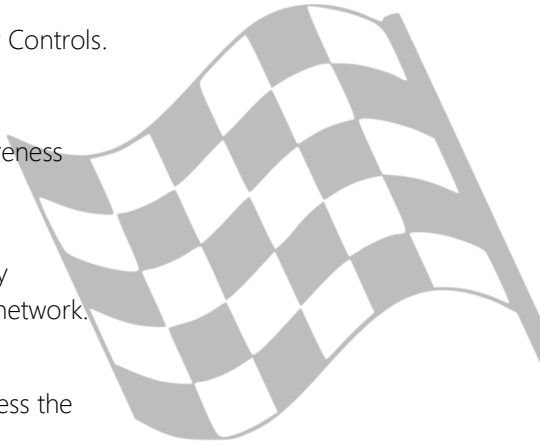
- [ ] Is there a record of data subject response to consent?
- [ ] Is there a record or log of data processing events involving personal data?
- [ ] Are these records secure and allow for queries, searches or reports by authorised personnel?
- [ ] Are policies kept current that describe how data processing is performed in compliance with the regulation?
- [ ] If a controller is outside the EU, is there a designated representative within the EU, and is this documented?
- [ ] If data processing services are contracted, does the legal agreement include the necessary clauses to ensure proper security and handling of personal data so as to be in compliance with GDPR?
- [ ] Is there sufficient access control to servers and buildings to prevent unauthorised individuals from accessing personal data?

Determine if data security practices and technology are adequate to meet GDPR requirements.

- ☐ Are appropriate technical and organisational measures taken to ensure that data is protected from accidental or unlawful destruction, loss, or alteration and unauthorised or unlawful storage, processing, access or disclosure?
- ☐ Does the security policy address the following?
  - How to protect data during storage and transmission.
  - How to restore access to data when an incident disrupts availability
  - How to ensure situational awareness of risks and enable preventative, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to data.
  - Describe the process for regularly assessing the effectiveness of security policies.
- ☐ Is there a process for providing breach notifications within 72 hours?
- ☐ Is there a record of a data protection impact Assessment (DPIA) assessing whether processing operations are likely to present specific risks?
- ☐ Was it completed within the last two years, or immediately when there was a change to specific risks in processing operations?
- ☐ Is there a designated DPO?

Tiedata's Managed Security appliances with Total Security Suite deliver the upgrade needed for compliance!

- ☐ **Strong overall security** that addresses 16 of SANS top 20 Critical Security Controls.
- ☐ **Threat Detection and Response** delivers data protection, situational awareness and automated remediation of threats.
- ☐ **Data Loss Prevention (DLP)** helps to prevent accidental data breaches by detecting and blocking files with personal information from leaving the network.
- ☐ **The portal** provides meaningful visualisation and reports that help to assess the effectiveness of security policies while anonymising any personal data.
- ☐ **Drag-and-drop VPNs** encrypt traffic between sites and are known for their stability.



Tiedata
Computing Solutions for Business...

Visit our website: www.tiedata.com