Composity

GENERAL DATA PROTECTION REGULATION (GDPR) COMPLIANCE CHECKLIST

Introduction

This checklist is based on the latest information available and highlights the areas you need to focus on, in order to prepare for compliance.

The General Data Protection Regulation - or the GDPR - regulates and protects the processing of personal information and ensures companies to be transparent about the data they handle and have a legitimate purpose for using it.

It establishes rules on how companies, governments and other entities can process the personal data of EU citizens or residents.

The regulation is enforced from 25th of May 2018 .

Awareness

- [ ] Ensure all key people are aware of the GDPR and its requirements.
- [ ] Determine whether and which of the GDPR requirements are applicable for your company.
- [ ] Consider whether a data protection officer (DPO) is required.
- [ ] Train all employees, who handle personal data, to handle it according to GDPR principles.

Information You Hold

- [ ] Review and document what personal data you hold, where it came from and who you share it with.
- [ ] Conduct a full risk assessment.
- [ ] Conduct a data protection impact assessment (DPIA) if required.

Consent & Legitimate Interests

- [ ] Establish legal basis for processing all the personal data that you hold.
- [ ] Make sure individuals are well informed of what you plan to do with their data when you collect it.

- [ ] Explain how or why you need an individual's personal data when you collect it.
- [ ] Keep a record of when and how you got consent from the individual.
- [ ] Name any third party organizations personal data may be shared with.
- [ ] Make sure that individuals can withdraw their consent.
- [ ] Regularly review consent and refresh it at appropriate intervals.
- [ ] Have transparent and easy to understand Privacy Policy and Terms of Uses.
- [ ] Adjust contracts, notices and policies to meet the new requirements.
- [ ] Use plain, simple and understandable language.
- [ ] Collect the minimum data necessary and delete records after use.
- [ ] Have a double opt-in procedure for registrations or subscribing users .
- [ ] Do not use pre-ticked boxes or any other type of consent by default.
- [ ] Give individuals the option to refuse marketing.

Individuals' Rights & Access

- [ ] Tell individuals about their right to have access to their own personal data rectificate or restrict it, that it is portable and can be deleted upon their request.
- [ ] Give individuals the tools to access, edit and delete their personal data.
- [ ] If an individual requires, you should transfer their personal data from one electronic system to another in readable format.

Security

- [ ] You have to have appropriate security measures to prevent data from being lost, stolen or disclosed to unauthorized people.

Hint: The GDPR specifically mandates both organizational and technical measures.

Some measures to consider:

- Pseudonymisation
- Encryption
- Ensuring ongoing integrity, confidentiality, availability and resiliency
- The ability to restore in a timely manner
- Control the access of employees and contractors

- [ ] Have procedures in place to report a breach within 72 hours of becoming aware of it.

Hint: If the breach is likely to result in a high risk to the rights and freedom of individuals, the company will need to notify all affected data subjects.

Notes