GDPR Compliance Checklist: Action Steps You Need to Take to Ensure Compliance

Complying with the Global Data Protection Regulation (GDPR) can seem overwhelming even for major global enterprises with robust internal resources capable of bringing it all to fruition. It can be difficult to determine where to start, but we've broken down the essential steps to GDPR compliance with an easy-to-reference checklist.

Background GDPR Preparation Action Steps

- **Awareness:** Take a deep-dive into the GDPR to gain an in-depth understanding of the new regulations and what's required for compliance.
- **Education:** Ensure that all decision-makers and key players within your organization are aware of the changes coming with GDPR and what it means for your organization.
- **Establish a Team:** Establish a GDPR implementation team to evaluate your company's needs and oversee the implementation of any changes that will need to take place in order to ensure compliance. This team should include representatives from each business unit who can then serve as liaisons with their respective departments.
- **Audit:** Perform an audit to document the personal information your company holds about EU residents, how the data is collected and from where, and any third parties that the data is shared with (such as third-party organizations that process your company's data).
- **Identify Your Lead Data Protection Supervisory Authority:** International organizations that operate in more than one member state or those that conduct cross-border data processing should identify their lead data protection supervisory authority for compliance and reporting purposes.
- **Review and Update Privacy Notices:** Most privacy notices currently in use by global organizations are insufficient for GDPR. Privacy notices must be clear and easily understood, and they must include all required information as outlined in the GDPR in order to obtain valid consent from data subjects.
- **Appoint or Hire a Data Protection Officer:** Determine whether your organization is required to hire a Data Protection Officer (DPO) under the GDPR. Some companies who are not required to do so may choose to appoint a voluntary DPO.
- **Address Record-Keeping Requirements:** Controllers are required to maintain thorough, accurate, and complete records pertaining to the personal data they collect, as well as how that data is processed, used, and stored. Audit your current record-keeping procedures and make changes and improvements as necessary.

- **Evaluate Data Retention Procedures:** Under GDPR, controllers are only permitted to maintain data about subjects as long as necessary for the purpose the data was originally obtained. Every company should evaluate their current data retention procedures, and many will need to make changes to their storage and retention processes to comply.

- **Conduct a Privacy Impact Assessment (PIA):** While not every company will be required to conduct a Privacy Impact Assessment, a PIA is necessary whenever new technologies are implemented that could result in a high risk to the rights and freedoms of individuals. Determine if your company needs to conduct a PIA, and carry out this process if required.

- **Employee Training:** All employees involved in the handling of personal data for other employees or customers must receive adequate training to ensure that they are aware of and follow appropriate data handling procedures. Keep records of training, and implement ongoing training to ensure that employees continuously follow appropriate data handling practices in accordance with GDPR.

- **Refresh Policies and Procedures:** Companies must establish a clear set of data protection policies, such as a general data protection policy, a checklist for responding to data breaches, policies related to the processing and retention of customer data, and policies related to privacy notices.

- **Implement Technical and Organizational Data Protection Measures:** Companies that collect or process personal data on EU residents must implement both technical and organizational measures to ensure adequate data protection based on the risk to individuals' rights and freedoms. These measures may include data minimization, encryption, and other measures that reduce the risks and protect data in a manner sufficient in the context of the type of data, the likelihood of risks, and the severity of potential risks.

- **Implement Procedures to Ensure That Only Necessary Data is Collected:** Under GDPR, companies must collect only the data that's necessary for the intended purpose. Companies must, therefore, implement technical and organizational measures that ensure that only the data necessary for each specific purpose are collected and processed, and that data is only stored as long as necessary for those purposes. These measures should also ensure that an individual's data is not made accessible to others without the explicit intervention of the individual.

Data Processing Action Steps

- **Establish a Legal Basis for Non-Sensitive Personal Data Collection:** Under GDPR, companies must have a legal basis for processing all non-sensitive personal data in order to ensure that all data is being processed lawfully.
- **Establish a Legal Basis for Sensitive Personal Data Collection:** Likewise, there must be an established legal basis for processing all special categories of personal data, otherwise known as sensitive data.
- **Determine if Consent is Required/Obtained:** If the legal basis for collecting personal data is consent, companies must ensure that valid consent is obtained and documented.
- **Address Profiling and Obtain Consent if Necessary:** For companies that profile employees or customers, in cases when profiling impacts decisions about those individuals, the company must obtain consent to conduct profiling.
- **Evaluate Data Collection on Children:** If your company collects data on children, ensure that privacy notices utilize appropriate language and that the appropriate procedures are in place for obtaining child consent.

Addressing the Rights of Data Subjects Action Steps

- **Establish Processes for Personal Data Requests:** If your company does not already have procedures in place to allow employees or customers to request a copy of their personal data, you must implement procedures to make it possible.
- **Ensure a Timely Response:** Companies must provide data subjects with the personal data collected on them, upon request, within one month following the request. Ensure that your organization has the staff and procedures necessary to comply with requests within this time frame.
- **Implement Technology and Processes to Support Individual Rights:** Data subjects have a number of other rights pertaining to their personal data, and companies must implement policies, procedures, and technologies that allow individuals to exercise those rights, including procedures to erase personal data promptly on request, procedures to correct inaccurate data, procedures to restrict data processing on request, and procedures to promptly provide individuals with the personal data your company has collected in a commonly used format.

Action Steps for Third-Party Processors and International Transfers

- **Establish Contracts with Third-Party Processors:** Companies that utilize third-party processors for processing personal data must establish clear contracts with those processors and ensure that all third parties have adequate data protection measures and procedures in place.

- **Evaluate and Address Compliance Issues with Data Transfers:** If your company transfers data outside the EU, ensure that only approved transfer mechanisms are used. Additionally, any third parties in receipt of transferred data are subject to GDPR compliance, and controllers must have confidence that adequate protection exists.

Breach Notification Action Steps

- **Implement Procedures for Prompt Mandatory Notification:** If a breach occurs, companies are required to notify the supervisory authority within 72 hours. Ensure that the necessary procedures are in place to ensure that breaches are reported to regulators within 72 hours of your company becoming aware of the breach. If notification occurs later than 72 hours after you've become aware of a breach, ensure that the eventual notice is accompanied by an explanation for the delay.

- **Determine When Notification to Data Subjects is Required:** In many cases, companies are required to notify individuals impacted by a breach in addition to the regulators. Notification to individuals is often not required when the data breached is encrypted or otherwise undecipherable by anyone without the proper authorization to access it. Your company should have a clear understanding of the circumstances under which data subjects must be notified.

- **Implement Procedures for the Prompt Notification of Data Subjects When Necessary:** Notifications of data breaches made to data subjects, when required, must occur promptly without unnecessary delay, and it must include specified information related to the type of data, the nature of the breach, and the steps the company has taken to address it. Ensure that your company has the staff and other resources necessary to promptly comply with notification requirements should a breach occur requiring data subjects to be notified.