GDPR Checklist

Steps Are Broken Into the Following General Categories:

1. Initial Steps For Beginning Your Compliance Efforts
2. Data Security
3. Vendor and Customer Contracts
4. Marketing
5. Employee Data Privacy

With the May 25th GDPR compliance deadline looming, company compliance efforts should be in full swing. Working towards complete GDPR compliance doesn't have to be an overwhelming task. Use this checklist to minimize anxiety; it breaks down the effort nicely into five categories with detailed steps. Each category provides steps companies should be taking, with descriptions, relevant GDPR articles and helpful resources for executing each task.

1 INITIAL STEPS

Determine Whether the Company is a Data Controller or a Data Processor

☐ Under the Article 4 of the GDPR, a data controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." Whereas a data processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." Unlike under the Data Protection Directive (DPD), under the GDPR the data controller and processor have separate duties. The controller's responsibilities are dictated in Articles 24–27 of the GDPR, while Article 28 outlines a data processor's duties under the GDPR. Because data controllers and processors have different duties, it is essential for companies to determine which entity they are. Companies need to realize that they can be both a controller and processor at the same time, depending on the data and the context.

Helpful Resources:
https://www.lexology.com/library/detail.aspx?g=9eabedfb-a61b-48b6-8985-e0728e2ffd8c
https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/

Conduct a Data Privacy Impact Assessment (DPIA)

☐ A DPIA assesses the impact of a particular processing operation on the protection of the personal data. While this is a good initial step to take to determine the protection of personal data when being processed, under Article 35 of the GDPR it is also required when a type of processing "is likely to result in a high risk to the rights and freedoms of natural persons." A DPIA is particularly required in the following three situations: (1) processing a large scale of special categories of data or personal data relating to criminal convictions and offenses; (2) an extensive and systematic evaluation, based on automated processing, of personal aspects relating to a natural person; and (3) systematic monitoring, on a large scale, of a publicly accessible area.

Helpful Resources:
http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Data%20Protection%20Impact%20Assessment%20under%20the%20GDPR.pdf

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Create Your "Record of Processing Activities"

☐ Under Article 30 organizations are required to keep records of data processing activities which include (a) name and contact details of controller, (b) purpose of processing, (c) description/category of data, (d) categories of recipients, (e) transfers to third countries, (f) general description of the organizational or technical measures. Organizations should compile the criteria required to be included in Article 37. Then run through your list of vendors and determine which vendors process personal data for you and if that data could be from an E.U.

citizen. If the answer is yes, record that data for the vendor. Many vendors will provide data protection agreements to help you through this task. Next, interview or audit your marketing, product, business development and HR functions to determine whether they collect personal data and ensure that you record those activities accurately.

☐ Some companies will also map how data flows through their systems to others, called a data map. A data map is not required by GDPR, but may be helpful (especially for organizations with complicated data processing activities or who use many third party sub-processors).

Begin a Vendor Audit to Ensure Vendors are GDPR Compliant

☐ Use your excel list to track compliance of vendors.

☐ Institute an assessment process to ensure all future vendors are compliant.

Determine Whether you are Required to Designate a DPO

☐ GDPR Article 37 requires a data controller or processor designate a DPO in any case where: (1) processing is carried out by a public body or authority, except when it is a court acting in its judicial capacity; (2) the controller or processor's core activities consist of processing operations that "require regular and systematic monitoring of data subjects on a large scale; or" (3) the controller or processor's core activities involve large scale processing of special categories of data and personal data relating to a criminal conviction or offense. Articles 38 and 39 of the GDPR go on to explain the required qualifications and responsibilities of a DPO.

Helpful Resources:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-2-the-mandatory-dpo/

http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-EU%20Data%20Protection%20Officer%20-%20Must%20Have,%20Nice%20to%20Have%20or%20Safe%20to%20Ignore.pdf

Employ a Cross-Border Data Transfer Mechanism

☐ Under Chapter 5 of the GDPR, controllers and processors must have in place a mechanism to provide adequate protection of personal data when transferring EU citizens' data outside of the EU. For transfers into the United States, this can occur through self-certifying under the EU-U.S. Privacy Shield Framework, employing European Commission approved standard contractual clauses, or using binding corporate rules.

Helpful Resources:
https://www.privacyshield.gov/welcome

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

2 DATA SECURITY STEPS

Put Proper Security Mechanisms in Place

☐ Article 32 of the GDPR requires both data controllers and processors to implement appropriate technical and organizational measures ensuring the security level appropriate to the associated risk. To determine what technical and organizational measures are appropriate, particular attention should be paid to the risks associated with processing the data, specifically: the "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed." Article 32 provides the following examples of appropriate technical and organizational measures: (1) pseudonymisation and encryption of personal data; (2) ability to restore availability and access to personal data in a timely manner after a breach incident; (3) process for regularly testing and evaluating the measures' effectiveness; and (4) "ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services."

Ensure your Technical Measures Enable your Company to Fulfill Data Subject Requests

☐ If the lawful basis for processing is consent of the data subject, then under the GDPR Articles 15, 16, 17, 18, 20, and 21, data subjects have more expansive rights regarding how companies process their data. These rights include: (1) the right of access to their data; (2) right to rectifying their data; (3) right to erasure of their data; (4) right to restrict processing of their data; (5) right to move their data from one processor to another; and (6) the right to object to the processing of their data. Data controllers and processors are required to employ technical measures to accommodate and execute these requests where the lawful basis for processing is consent.

Update Data Breach Notification Policies

☐ Articles 33 and 34 address the procedures that must occur when a data breach occurs. Article 33 requires data controllers to notify the Supervisory Authority of a data breach no later than 72 hours after becoming aware of the breach. Processors are required to alert the data controller of a data breach without undue delay upon becoming aware of the data breach. Article 34 dictates that the data controller must notify the data subject, without undue delay, when a data breach is "likely to result in a high risk to the rights and freedoms of natural persons."

Helpful Resources:
https://www.jdsupra.com/legalnews/article-29-working-party-issues-revised-75873/
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/

Update Incident Response Plan

☐ Company incident response plans should be updated to reflect the new data breach notification procedures and timelines indicated in Articles 33 and 34 of the GDPR.

Helpful Resources:
https://www.jdsupra.com/legalnews/article-29-working-party-issues-revised-75873/
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/

3 VENDOR & CUSTOMER CONTRACT STEPS

Update Mandatory Contractual Provisions

☐ Review Current Contracts for Required Provisions

☐ Create Vendor GDPR Data Protection Amendments

☐ Under Article 28(3) of the GDPR, agreements between controllers and processors must include specific contractual language. The agreement must set out "the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller." Article 28(3) then goes on to stipulate eight specific provisions to be included in these agreements.

Create a GDPR Data Protection Amendment for Your Customers

☐ Under GDPR Article 13, data controllers must be transparent with data subjects about processing activities when collecting data subjects' personal data. Article 13 paragraphs 1 and 2 provide a list of information that must be provided to these data subjects. For example, data subjects must be provided with how long their data will be retained, that they have the right to lodge complaints with the Supervisory Authority, the existence of their rights as data subjects, the identity of the controller, contact details for the data controller's data protection officer, in addition to other pieces of information.

Helpful Resource:
https://gdpr-info.eu/art-13-gdpr/

4 MARKETING STEPS

Update the consent language on your website

☐ Opt-in Consent and outline data being collected and the purposes for processing

☐ Under its definition in Article 4(11) of the GDPR, consent must be (1) freely given, (2) obvious and require an affirmative action to opt in; (3) specifically cover the controller's names, processing purposes, and processing activities; and (4) informed and unambiguous.

Helpful Resources:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

https://ico.org.uk/for-organisations/marketing/

Update Social Media Data Collection Notice

☐ While currently not required, an October 24, 2017 German preliminary ruling determined that under Germany's DPD implementing legislation, an administrator of a fan page on a social media site "must be regarded as being a controller, within the meaning of that provision, in so far as concerns the phase of personal data processing consisting in the collection by that social network of data relating to people who visit the fan page for the purpose of compiling viewing statistics for that fan page." It is speculated that this interpretation, if the case ultimately becomes binding precedent, would apply to the controller definition in the GDPR. To address this possibility, companies should include a notice at the top of all social media pages stating that the social media site also collects and processes user data and linking to the social media site's privacy policy.

Helpful Resource:
https://www.courthousenews.com/wp-content/uploads/2017/10/facebook-ireland.pdf

5 EMPLOYEE DATA STEPS

Update Consent Language on EU Employee Contracts & Job Applicant Forms

☐ According to the Article 29 Data Protection Working Party (Working Party) Opinion of data processing at work, employees are rarely in a position to freely give, refuse, or revoke consent based on the dependency between an employee/employer relationship. Due to this, employees can only freely give consent in exceptional circumstances. Therefore, companies are more likely to be able to rely on the lawful basis of legitimate interest for processing employee personal data. However, it is still important for companies to include consent language in their employee contracts and job application forms.

Create a Template Data Processing Transparency Notification

☐ GDPR Article 88 and the Working Party opinion on data processing at work, companies are required to provide effective communication to employees regarding (1) any monitoring that takes place, (2) purposes and circumstances for the monitoring, and (3) any ways employees can prevent their data being collected by the monitoring technologies.

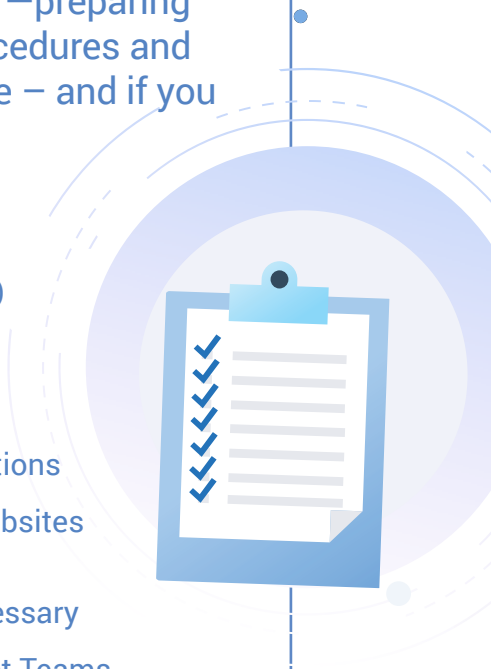
Helpful Resources:

https://iapp.org/news/a/wp29-releases-extensive-employee-privacy-guidance/

https://www.taylorwessing.com/globaldatahub/article-processing-of-hr-data-under-the-gdpr.html

For the full guidance go to the following link and scroll down to WP 249 under Letters, Opinions and Other Documents:
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

GDPR is not a trivial exercise. Just like data security itself—preparing for GDPR needs to be embraced with proper policies, procedures and technologies put in place. Let this checklist be your guide – and if you need to start smaller, here are the **top 8 Must-Do steps:**



- ✓ Create or Update Your "Record of Processing Activity"
- ✓ Determine Whether to Designate a Data Protection Officer (DPO)
- ✓ Update Mandatory Contractual Provisions
- ✓ Employ a Cross-border Data Transfer Mechanism
- ✓ If You Process Data Based on Consent, Understand Your Obligations
- ✓ Update Privacy Notices and Consent Language on Company Websites and Social Media Pages Where You Collect Personal Data
- ✓ Make Sure You Can Delete / Destroy Data When No Longer Necessary
- ✓ Embed Your Privacy Experts with Your Development and Product Teams

Don't Run Out of Time

May 25th is only weeks away. Don't risk running out of time to properly implement a comprehensive compliance solution. There are market opportunities and competitive advantages for firms that prepare in advance, in contrast to potential revenue loss and reputation damage for those that fail to plan.

To learn more about how Smarsh can help your organisation prepare for GDPR call +44 (0) 800 048 8612 or visit **The Archiving Platform** on www.smarsh.eu, and watch a demo of how the platform works.