Fox Rothschild LLP
ATTORNEYS AT LAW

ARE YOU GDPR COMPLIANT?

The General Data Protection Regulation (GDPR) applies to any business that collects, processes, stores or uses:

- personal data of any European Union (EU) citizen
- personal data collected in Europe
- personal data transmitted to or from Europe
- personal data received from customers or vendors that is subject to EU law

The regulation defines personal data very broadly to include identifiers such as names, identification numbers, location data, online identifiers or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
The GDPR has onward compliance requirements. If your business provides services to a business that must comply with GDPR, then your business is also likely to face some GDPR requirements.

Even if your vendor contracts comply with existing law under Data Protection Directive 95/46/EC, they may need to be updated to comply with specific GDPR requirements, such as obligations in Articles 32 to 36 pertaining to assistance with data breach notification and conducting data protection impact assessments.

ORIGINS

The GDPR replaced Data Protection Directive 95/46/EC. It was created to provide a single data privacy law for the European Union (EU), to provide guidance and uniformity in how businesses approach and handle data privacy and protect the personal data of EU citizens from misuse and loss.

GDPR took effect on May 25, 2018.

TO WHOM DOES IT APPLY

The GDPR applies to businesses inside and outside the EU. Any business that collects, processes or holds EU citizens' personal data must comply with the GDPR regardless of where the business is located.

Fox Rothschild LLP
ATTORNEYS AT LAW

Are You GDPR Compliant?

WHAT IS PERSONAL DATA?	The GDPR applies to businesses inside and outside the EU. Any business that collects, processes or holds EU citizens' personal data must comply with the GDPR regardless of where the business is located.
CONTROLLERS VS. PROCESSORS	The GDPR differentiates between controllers and processors of personal data. The controller is the party that alone, or jointly with others, determines the purposes and means of processing personal data. The processor is the party that processes personal data on behalf of the controller.
NOTIFICATION REQUIREMENTS	If a data breach results in a loss of personal data, the controller must notify the affected party's controlling supervisory authority without undue delay and, where feasible, no later than 72 hours after learning of the breach. This does not apply if the loss is unlikely to result in a risk to the rights and freedoms of natural persons. Processors that discover a personal data breach must notify controllers without undue delay.
HIGH RISK BREACH	In situations where a personal data breach is likely to result in a high risk to the rights and freedoms of affected individuals, the controller shall inform the data subject of the breach without undue delay.
INDIVIDUAL CONSENT	If relying on consent to process personal data, a controller must be able to demonstrate that individual's consent. Consent must be sought in an intelligible and easily accessible manner, using clear and plain language. If consent is requested in written materials that deal with other matters, the request for consent must be clearly distinguishable from the other matters. An individual shall have the right to withdraw his or her consent at any time. Before giving consent, an individual must be notified of their right to withdraw consent. The process of withdrawing consent must be as easy as the process to grant consent.

Fox Rothschild LLP
ATTORNEYS AT LAW

Are You GDPR Compliant?

SENSITIVE DATA	**If sensitive data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data – is collected, consent must be explicit, nothing less than an opt-in. Consent for personal data collection must be unambiguous.**
PENALTIES	**The GDPR imposes significant penalties on violators. Fines for technical non-compliance, such as failure to make a breach notification or conduct an impact assessment, may be as high as the greater of €10 million or 2 percent of global annual turnover (revenue) from the prior year. Fines for non-compliance with certain key provisions of the GDPR, such as insufficient consent or violating privacy by design, can reach up to the greater of €20 million or 4 percent of global annual turnover in the prior year.**
MINORS & PARENTAL CONSENT	**Parental consent will be required in order to process the personal data of children younger than 16. Countries have the option to lower the age of consent to as low as 13.**
DATA PROTECTION OFFICER	**The controller and processor must designate a data protection officer for any case in which:** • Processing is carried out by a public authority or body, except for courts acting in their judicial capacities. • The core activities of the controller or processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. • The core activities of the controller or the processor consist of large scale processing of special categories of data and personal data relating to criminal convictions and offenses.

Fox Rothschild LLP
ATTORNEYS AT LAW

GDPR Check

ASSESSMENT OVERVIEW

This assessment maps your organization's data management practices in 17 areas that are key to determining GDPR compliance, producing a report for each that you can save and/or share with others.

SECTION 1: Types of Data Collected; Company Demographics

Consider all countries in which your company operates, how data is processed in each and whose data is being processed where. Think about all the types of data collected by or on behalf of your company, and the countries of citizenship of the individuals from whom you collect or receive data. This includes customers, employees and any other person whose individual data you receive. Identifying this data and its origin is the first step to understanding your compliance obligations.

Does the company collect data about consumers, patients, employees or other individuals?

- ☐ Yes
- ☐ No

If yes, what types of data does the company collect? (Check all that apply)

- ☐ Name/Address/Contact Information
- ☐ Social Security Number, State ID, Passport Number, etc.
- ☐ Health Information
- ☐ Financial, Account or other Transactional Data
- ☐ IP Address
- ☐ Device ID (such as MAC Address)
- ☐ Other Digital Signatures/Digital IDs
- ☐ Genetic Information or other Biometric Information
- ☐ Usernames/Passwords
- ☐ Race/Ethnicity
- ☐ Age
- ☐ Gender
- ☐ Sexual Preference
- ☐ Religious Beliefs or Affiliations
- ☐ Political Opinions, Membership or Affiliation
- ☐ Labor/Trade Union Membership
- ☐ Criminal or Arrest Records
- ☐ Judgments or Legal Action
- ☐ Credit Scores, Credit Worthiness, etc.
- ☐ Level of Education
- ☐ Job Status, Job Title, Salary or Employment Information
- ☐ Other Identifying Information

Does the company use employee information to administer health benefits or other employee benefits?

- ☐ Yes
- ☐ No

GDPR Check

Does the company have unionized employees?

- ☐ Yes
- ☐ No

In which industries does the company operate? (check all that apply)

- ☐ Automotive
- ☐ Childcare or other Industries Oriented Toward Minors
- ☐ Defense
- ☐ Education
- ☐ Energy
- ☐ Entertainment
- ☐ Financial Services/Banking
- ☐ Food & Beverage
- ☐ Healthcare/Life Sciences/Pharmaceutical
- ☐ Insurance
- ☐ Manufacturing
- ☐ Professional Services
- ☐ Real Estate/Construction
- ☐ Retail/Consumer-Oriented
- ☐ Technology
- ☐ Telecommunications
- ☐ Transportation (Airlines, Trucking, Shipping, etc.)
- ☐ Other

GDPR Check

SECTION 2: Privacy Policies and Other Notices

Privacy policies and similar notices inform individuals of how you collect, store, use, share and discard data. The content of these documents should be updated often to conform to new legal requirements and organizational changes.

Does the company provide notice to individuals about its data collection policies?

- Yes
- No

Do you maintain a written Privacy Policy?

- Yes
- No

Is the Privacy Policy public facing?

- Yes
- No

Is the Privacy Policy written in clear/plain language?

- Yes
- No

Does it clearly articulate the character, types and categories of data that the company collects, processes, stores and shares/discloses?

- Yes
- No

Is the Privacy Policy conspicuous, easy to find and separate from other policies available to the public?

- Yes
- No

Does the company maintain separate policies for different product/service offerings?

- Yes
- No

Is the Privacy Policy available both online and in any mobile application, if applicable?

- Yes
- No

Does the Privacy Policy - or each policy - include the right to object to the collection of personal data? (i.e., front-end opt-out)

- Yes
- No

Does the Privacy Policy include the right to withdraw consent for the collection of data? (i.e., back-end opt-out)

- Yes
- No

Does the privacy policy allow the company to unilaterally change the policy and the manner in which it uses personal data?

- Yes
- No

GDPR Check

Does the company use personal data for direct marketing or tasks in the public interest/ legitimate interest?

- Yes
- No

Does the company explicitly draw the attention of data subjects to the specific uses separately from other information/notices?

- Yes
- No

Will an individual lose access to the services if the individual revokes consent for the specified collection, process, use and/or disclosure of the individual's personal data?

- Yes
- No

If yes, does the Privacy Policy specify that an individual will lose access to the services if the individual revokes consent to their personal data?

- Yes
- No
- N/A

Does the company maintain internal Privacy Policies or other notices affecting or targeted at employees?

- Yes
- No

If yes, are such policies included in employment contracts, employee handbooks, etc.?

- Yes
- No
- N/A

Are employees required to consent to the company sharing their personal data with vendors or other providers of the company, such as employee benefits providers?

- Yes
- No

Does the company share employee personal data with third-party partners for the purpose of providing special offers, services or other marketing activities geared to employees?

- Yes
- No

GDPR Check

SECTION 3: Consent

Businesses in certain industries are required to obtain consent from each individual to collect and use their personal data. In other industries, a business may, but is not required to seek consent before using personal data. Understanding your practices for each collection method will help you formulate the best mechanisms for obtaining consent under the GDPR.

"Legitimate interests" include: a) processing for direct marketing purposes or preventing fraud; b) transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data; c) processing for the purposes of ensuring network and information security, including preventing unauthorized access to electronic communications networks and stopping damage to computer and electronic communication systems; and d) reporting possible criminal acts or threats to public security to a competent authority.

How does the company obtain consent for collection, use and disclosure of their personal data (i.e., click-wrap, written statement, other acknowledgement, etc.)?

Is consent required from the individual data subject for collection, processing, use and/or disclosure of personal data (i.e., are products or services provided on an opt-in basis)?

- Yes
- No

Is the data subject required to take an affirmative step to provide consent (i.e., click a box, enter a code, etc., versus silence, pre-ticketed boxes, inactivity, etc.)?

- Yes
- No

Is personal data from the data subject necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract?

- Yes
- No

Is personal data from subject necessary for compliance with a legal obligation?

- Yes
- No

Is personal data from data subject necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent?

- Yes
- No

Is personal data from data subject necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the company?

- Yes
- No

GDPR Check

Does the company rely on "legitimate interests" for lawful processing of personal data? *See above for more on "legitimate interests."

- Yes
- No

Does the Privacy Policy identify the legitimate interests?

- Yes
- No

Is personal data used for direct marketing purposes or to prevent fraud?

- Yes
- No

Is personal data, including client and employee data, used for internal administrative purposes?

- Yes
- No

Is personal data used for the purposes of ensuring network and information security, including preventing unauthorized access to electronic communications networks and stopping damage to computer and electronic communication systems?

- Yes
- No

Is personal data used for reporting possible criminal acts or threats to public security to a competent authority?

- Yes
- No

Are separate consents obtained for distinct processing operations (i.e., separate consent for using personal data to open a checking account versus use of personal data to perform direct marketing for mortgage products by a third party)?

- Yes
- No

Does the company process sensitive data (i.e., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, sex life or orientation data, generic data, biometric data)?

- Yes
- No

Does the company obtain consent of the data subject when processing sensitive data?

- Yes
- No

Is personal data necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement?

- Yes
- No

Is personal data necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent?

- Yes
- No

GDPR Check

Is personal data processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members?

- Yes
- No

Is personal data manifestly made public by the data subject?

- Yes
- No

Is personal data necessary for the establishment, exercise or defense of legal claims or where courts are acting in their judicial capacity?

- Yes
- No

Is personal data necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued?

- Yes
- No

Is personal data necessary for the purposes of preventative or occupational medicine, accessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional?

- Yes
- No

Is personal data necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medical products or devices?

- Yes
- No

Is personal data necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes (See Article 89(1))?

- Yes
- No

Do you have appropriate safeguards in place to address the purposes outlined above for use of personal data?

- Yes
- No

GDPR Check

SECTION 4: Territorial Scope

If you are collecting personal data from EU citizens, it is important to have a detailed understanding of how the GDPR views your use of their personal data.

"Offering of Goods or Services"

In considering whether your company is "offering goods or services" to subjects in the EU, the following factors are relevant:

1. Insufficient to constitute "offering:"
   a. Mere accessing is insufficient. It must be apparent your company "envisages" that activities will be directed to EU data subjects
   b. Using your own country's language and mere accessibility by data subjects in EU is generally insufficient.
2. Relevant:
   a. Using EU language/currency
   b. Ability to place orders in other languages
   c. References to EU users/customers
   d. Payment of money to search engines to facilitate access to EU data subjects
   e. International nature (e.g., tourist activities, telephone numbers with an international area code, use of .de or .eu domains, mentions of international clientele for EU, descriptions of itineraries from EU to place where service is provided, etc.)

"Monitoring Behavior"

Specifically includes the tracking of individuals online to create profiles, including where it is used to make decisions to analyze/predict personal preferences, behaviors and attitudes.

International Transfers

If your company processes personal data of EU subjects from ***outside the EU***, pay close attention to Section 17, regarding international transfers.

Are you processing personal data of subjects in the EU?

- Yes
- No

Are you processing personal data in connection with the "offering of goods or services" (payment not required)?

- Yes
- No

Are you processing personal data in connection with "monitoring" the behavior of data subjects within the EU?

- Yes
- No

Does your company process personal data of data subjects in the EU pursuant to an employment relationship?

- Yes
- No

GDPR Check

SECTION 5: Personal Data Inventory (Data Mapping)

This section focuses on how you, and the vendors your company works with, track and map the flow of managed personal data. Data mapping is a significant undertaking for any business, but it is crucial for understanding what data your business has and where it is located. These questions will help you develop a data map overview.

Has the company inventoried the personal data it collects from individuals, including type of personal data and where it is stored?

- Yes
- No

Has the company inventoried how the personal data it collects from individuals is being used?

- Yes
- No

Is the company collecting, storing or maintaining more personal data than necessary to provide the product/service to individuals?

- Yes
- No

Has the company inventoried with whom the personal data it collects from individuals is being shared?

- Yes
- No

Does the company have a comprehensive data map showing the flow of personal data within and out of the company?

- Yes
- No

Have all personal data flows from the EU into the US been mapped?

- Yes
- No

Does the company maintain/implement a comprehensive vendor management program?

- Yes
- No

Are vendors subject to a security questionnaire or other assessment before working with the company?

- Yes
- No

Are vendors subject to any specific standards or policies for privacy, security or compliance with laws?

- Yes
- No

Are vendors audited periodically, including privacy and security audits?

- Yes
- No

Are vendors instructed or otherwise limited (by contract or otherwise) to processing personal data on behalf of the company only in compliance with instructions or direction from the company?

- Yes
- No

Does the company use or otherwise commercialize anonymized, de-identified and/or aggregated data derived from the personal data it collects?

- Yes
- No

GDPR Check

SECTION 6: Internal Privacy Policies

This section examines your organization's readiness to address policy. It's important to tell the world about your personal data practices, but it is equally important that the individuals responsible for safeguarding data and ensuring it is used responsibly understand your business's philosophy and policies.

Does the company have technical and organizational procedures and policies in place to protect and secure collected personal data?

- Yes
- No

Does the company train and provide continuing education to personnel on its internal privacy policy?

- Yes
- No

Does the company exercise, drill or otherwise test its readiness and/or ability to implement internal policies?

- Yes
- No

Does the company periodically (at least annually) test, assess or audit its performance or compliance with policies or external/ industry standards?

- Yes
- No

If yes, are audits performed by internal or external personnel, and are audit reports issued and retained?

- Yes
- No

Are internal policies extended to contractors or other personnel or entities, or do they apply to employees only?

- Yes, policies extend to contractors or other personnel.
- No, policies apply to employees only.

GDPR Check

SECTION 7: Data Retention and Disposal

An appropriate data retention policy and corresponding practices ensure that you know what data you have and that you keep it only for as long as necessary.

Aside from the below, you should also consider:

- How your data is disposed of after use or after expiration of your retention period.
- How much of your data is considered "dark," "unstructured," "slack," "legacy" or otherwise unknown or unused.

Does the company have a data retention policy or other similar policy?

- Yes
- No

Does the retention policy consider whether the purpose for which the data was collected or processed is still necessary?

- Yes
- No

Are retention periods tied to specific regulatory or contractual retention periods, to best practices, neither or both?

- Defined by regulation/contracts
- Defined by best practices
- Neither
- Both
- Not Applicable

Does the company notify employees, consumers or other data subjects of the data retention policy?

- Yes
- No

Does the data retention policy address situations where personal data is no longer necessary for the purpose for which it was collected or processed?

- Yes
- No

Does the data retention policy address situations where personal data was not collected in a lawful manner?

- Yes
- No

Does the data retention policy address situations where personal data was made public?

- Yes
- No

Does the data retention policy include notice provisions for other companies who are processing the data?

- Yes
- No

Are data retention and deletion standards included in vendor agreements or as part of a vendor management program?

- Yes
- No

Does the company maintain data in legacy or decommissioned systems, store/keep/have dark data (i.e., operational data not being used or that is unknown/unidentified), or other unstructured data?

- Yes
- No

SECTION 8: Uses of Personal Data (Processing, Access, Modification, Return, Objection and Deletion)

Describing to individuals how their personal data is used is a best practice and is required under the GDPR, as well as the laws of some US states.

- *Outside of the Privacy Policy addressed in Section 2, how does the company provide data subject with information regarding the purposes and legal basis for processing personal data (i.e., are there product- or service-specfic terms, in-service disclosures or other methods used)?*
- *What level of specificity is provided to your data subject in regards to the identities of recipients of their data?*
- *How and where are notices made available?*
- *What kind of access controls or other limitations are implemented when restricting processing of personal data?*

Regarding data transfers outside the EU:

- *How much information is provided to data subjects?*
- *Which data transfer mechanism is used to protect personal data? (see Section 17 for more)*

Does the company provide the data subject with the identities of (third-party) recipients, or categories of recipients who might receive the data?

- Yes
- No

Are there recipients or categories of recipients not included in the Privacy Policy or other notice(s) to individuals?

- Yes
- No

Does the company provide the categories of information and the source(s) from which it collects personal data, including if it came from publicly accessible sources?

- Yes
- No

Does the company provide the data subject details on data transfers outside the EU?

- Yes
- No

Does the company identify how a data subject can obtain a copy of the company's Binding Corporate Rules, see the company's Privacy Shield certification or identify other safeguards?

- Yes
- No

Does the company's system allow a data subject to obtain confirmation of whether his/her personal data are being processed?

- Yes
- No

GDPR Check

Does the company clearly articulate how and where to send such requests?

- Yes
- No

Can requests be processed within one (1) month of the request?

- Yes
- No

Does the company's system allow data subjects to request access to personal data collected/stored/processed by the company?

- Yes
- No

Does the company's system allow data subjects to request modification of personal data collected/stored/processed by the company?

- Yes
- No

Does the company's system allow data subjects to port personal data from the company to a competitor in a digital format?

- Yes
- No

Does the company's system allow data subjects to port personal data from the company to a competitor using standard formats (rather than proprietary)?

- Yes
- No

Does the company's system allow data subjects to request personal data be deleted/eradicated (Right to be Forgotten)?

- Yes
- No

Is there a charge for obtaining a copy of the data processed?

- Yes
- No

Is personal data replicated (for backup, record keeping, or otherwise)?

- Yes
- No

Upon request for deletion, does the company forward the request to companies replicating data (such as DR, COOP or other backup)?

- Yes
- No

Does the company's system track or record when a data subject has withdrawn consent?

- Yes
- No

Does the company assess and record whether there is no longer any justification (including legitimate interest) for processing?

- Yes
- No

If there is no longer a justification for maintaining the personal data, does the company delete the data?

- Yes
- No

Is there a simple method for withdrawing consent, including methods using the same medium used to obtain consent (e.g., website, email, text, etc.)?

- Yes
- No

GDPR Check

Does the company's system allow an individual to receive their personal data back in a commonly used format?

- Yes
- No

Does the company notify data subjects that they can complain to a supervisory authority for improper collection, processing, storage, use or disclosure of personal data, whether in the Privacy Policy or otherwise?

- Yes
- No

Does the company notify data subjects if there is a statutory or contractual requirement to provide data, and the consequences of not providing the data?

- Yes
- No

Does the company ever further process previously collected personal data?

- Yes
- No

Does the further processing have a new purpose (for example, an insurance company using past claims data to market new insurance products to insureds)?

- Yes
- No

Is the further processing based on consent?

- Yes
- No

When further processing personal data, is the new purpose compatible with the original purpose?

- Yes
- No

Does the company archive personal data?

- Yes
- No

Are the archiving purposes:

- in the public interest
- for scientific and historical research purposes
- for statistical purposes

Does the company restrict processing of personal data when applicable?

- Yes
- No

Are restrictions applied when a data subject disputes the accuracy of data?

- Yes
- No

Are restrictions applied when a data subject has objected to the company's processing/use of personal data?

- Yes
- No

Are restrictions applied when processing is unlawful, when a data subject objects to deletion and requests restriction instead?

- Yes
- No

Are restrictions applied when the company has no further need for data, but personal data is required to establish, exercise or defend legal claims?

- Yes
- No

GDPR Check

SECTION 9: Automated Processing of Personal Data

The GDPR imposes special prohibitions and requirements on businesses that use any automated process to make decisions. These questions will help you understand if you are subject to these additional prohibitions and requirements.

Does the company evaluate or make decisions with regard to a data subject based on automated processing, including profiling?

- Yes
- No

Does such processing require explicit consent from the data subject(s)?

- Yes
- No

Is there a right to obtain human intervention to allow the data subject to express his/her point of view and/or to consent to any automated processing decision(s)?

- Yes
- No

Are you aware whether automated processing was authorized by Member State law/EU law for the particular purpose or type of processing performed?

- Yes
- No

Is automated processing necessary to enter into, or to perform, a contract between a data subject and the company?

- Yes
- No

Does the data processed include sensitive information?

- Yes
- No

If the data processed includes sensitive information, was explicit consent received from the data subject?

- Yes
- No

Is processing necessary for substantial public interest reasons and on the basis of Member State/EU law?

- Yes
- No

GDPR Check

SECTION 10: Vendors and Subcontractors

Requirements governing the use of personal data by a business's vendors and subcontractors are among the most overlooked aspects of the GDPR. Not only must an affected business comply with the GDPR, but so must the vendors and subcontractors that process personal data on its behalf.

Does the company use vendors, subcontractors or other third parties to process (or as a sub-processor of) individual personal data?

- Yes
- No

Does the company have a subcontractor risk management program?

- Yes
- No

Does the company have agreements in place with its subcontractors that restrict appointment of sub-processors without the company's consent?

- Yes
- No

Are you aware whether automated processing was authorized by Member State law/EU law for the particular purpose or type of processing performed?

- Yes
- No

Does the company have agreements or policies that restrict vendors or subcontractors from processing, storing, using, or disclosing personal data without the company's consent or direction (or only at the direction of the company)?

- Yes
- No

Can the company identify all vendors, subcontractors or other third parties that receive personal data from or through the company?

- Yes
- No

Can the company identify where vendors, subcontractors or other third parties processing personal data are located (or where processing activities take place)?

- Yes
- No

Can the company identify the classifications, types, and/or volume of personal data transferred to each vendor, subcontractor or other third party?

- Yes
- No

Are all vendors, subcontractors or other third parties working on behalf of the company subject to confidentiality and/or non-disclosure language?

- Yes
- No

GDPR Check

SECTION 11: Breach Readiness and Response

The GDPR includes a large breach notification and response component. In order to meet these obligations adequately and in a timely manner, a business must have appropriate plans and procedures in place.

A "data controller" is usually the company's customer or source of the personal data.

Some important questions to consider:

- *What is the time limit for notification of data controllers?*
- *What is the time limit for notification of supervisory authority (government regulators)?*
- *What is the time limit for notification of the data subject?*
- *What types of data breaches are reported? All incidents? Only material incidents?*

Does the company have a cyber incident or data breach response and notification plan?

- Yes
- No

Does the plan have a time limit to notify applicable regulator, data controller, and/or other parties in the event of a breach?

- Yes
- No

Does the company document each security incident?

- Yes
- No

Does the company employ any Security Information and Event Management (SIEM) tools or other similar hardware or software programs?

- Yes
- No

Does the incident documentation process include facts relating to the nature of the personal data breach, or method in which the breach occurred?

- Yes
- No

Does the incident documentation process include the scope of the breach (number of individuals affected, systems affected, and/or type of information accessed or compromised)?

- Yes
- No

Does the incident documentation process include the remedial actions taken (both on behalf of individuals and by the company)?

- Yes
- No

Does the company practice its data breach response and notification plan?

- Yes
- No

How often does the company practice its data breach response notification plan?

How often is the company's data breach and response plan updated?

GDPR Check

Who is the control group in the Incident or Breach Plan? Which employees are responsible and are roles clearly defined?

Does the company maintain cyber-liability insurance coverage?

- Yes
- No

Is the company aware of exclusions from the policy?

- Yes
- No

Has the company analyzed any exclusions relative to actual operations?

- Yes
- No

Does the company have outside providers (such as attorneys, security consultants, accountants, forensic experts, etc.) identified and retained to assist in a rapid response in the event of an incident?

- Yes
- No

SECTION 12: Complaints and Sanctions

Creating an environment that encourages positive and negative feedback about privacy and security practices not only increases engagement, it results in better practices.

Does the company have a complaint handling policy and process?

- Yes
- No

Is the policy internal, external or both?

- Internal
- External
- Both

Has the company identified an alternative dispute resolution mechanism for complaints (e.g. arbitration via AAA, JAMS, BBB, Truste, etc.)?

- Yes
- No

Does the company make contact information available or have another mechanism for individuals to direct complaints or other concerns to the company?

- Yes
- No

Does the company have a policy for imposing sanctions or discipline on personnel who violate the company's privacy or security policies?

- Yes
- No

If the company maintains cyber-liability insurance, does it cover regulatory enforcement actions, fines, or other costs/penalties which may be associated with administrative proceedings related to a complaint filed with a Data Protection Authority or other government agency?

- Yes
- No

SECTION 13: Data Protection Officer and EU-Based Representatives

The GDPR requires many organizations to appoint a Data Protection Officer and designate individuals for dealing with the local Data Protection Authority. The regulation lists specific requirements and makes recommendations for ensuring appointment of the proper individual.

Has the company appointed or hired a data protection officer (DPO)?

- Yes
- No

Does the DPO have operational IT responsibilities?

- Yes
- No

Does the DPO have expert knowledge of data protection law and practices?

- Yes
- No

Are the contact details of the DPO made available internally and externally?

- Yes
- No

Has the company appointed an EU-based representative?

- Yes
- No

SECTION 14: Privacy Impact Assessments

A Data Privacy Impact Assessment (DPIA) is an assessment of privacy risks posed to individuals by the collection, disclosure and use of their personal data. Under the GDPR, controllers must conduct DPIAs when the risk of a privacy breach is high, in order to minimize the risks to data subjects.

Does the company have a policy/procedure for conducting a Privacy Impact Assessment (PIA) for new data collection/use or changes to data collection/handling/use to address data protection and privacy concerns?

- Yes
- No

Does the PIA include a description of the processing activities and their purpose?

- Yes
- No

Does the PIA include an assessment of the need for and proportionality of the processing?

- Yes
- No

Does the PIA include an assessment of the risks arising from the processing and measures adopted to mitigate those risks?

- Yes
- No

Does the PIA include an assessment of safeguards and security measures to protect personal data and the company under GDPR?

- Yes
- No

Did the DPO advise on carrying out the PIA?

- Yes
- No

Are supervisory authorities consulted before initiating processing activities involving high levels of unmitigated risks found by a PIA?

- Yes
- No

SECTION 15: Record of Processing Activities

Under the GDPR, a business must keep an accurate record of its personal data processing activities. How and where are such records stored? What content is included in the records?

Does the company keep a record (or log) of its processing activities?

- Yes
- No

Does the record include the type of data processed?

- Yes
- No

Does the record include the purpose for processing the data?

- Yes
- No

Are the records automatically or manually created?

- Yes
- No

SECTION 16: Minors

Parental consent will be required to process the personal data of children under age 16. Countries have the option to lower the age of consent to as low as 13. Your company may already comply with laws covering such data, but you also may have received data unintentionally. Consider the methods and mechanisms used to verify parental consent. Think about your efforts to track, update, modify and keep parental consent current. Consider your efforts to segregate, track and protect personal data related to minors.

Is the company collecting personal data from children under the age of 16?

- Yes
- No

Is the company making reasonable efforts to verify parental consent?

- Yes
- No

Are any notices addressed to children written in a clear and plain language that the child can easily understand?

- Yes
- No

Does the company employ any policies, technical or otherwise, to segregate, track, or otherwise protect personal data related to minors?

- Yes
- No

GDPR Check

SECTION 17: International Transfers of Data

The transfer of personal data across borders raises unique issues, depending on the country of export or import. You should consider all locations to which your data may travel or be transferred.

Binding Corporate Rules (BCRs)

- *In what member states have BCRs been approved?*
- *Which divisions, functions, transfers or categories of data do the BCRs cover?*

Model Contract Clauses

- *In what instances/for what relationships does the company use MCCs for international data transfers?*
- *Is the company a Controller, Processer, Sub-Processor, or more than one of the above pursuant to the MCCs it has in place?*
- *Does the company maintain or use a data transfer agreement, data processing agreement, or other similar agreement in addition to any MCCs?*

Privacy Shield

- *Is the company US-EU and/or US-Swiss Privacy Shield Certified?*
- *Where is the company's Privacy Shield policy available?*
- *Does the company self-assess or use outside auditors for compliance?*
- *Has the company selected an ADR mechanism? Which one?*
- *Does the company have downstream agreements or notices with vendors that obligate the vendors to protect personal data in a manner consistent with the Privacy Shield?*

Does the company transfer data about EU citizens or about data subjects collected, processed, or stored within the EU, to itself or other third parties located outside the EU?

- ☐ Yes
- ☐ No

Which of the following transfer mechanisms are used? Mark all that apply:

- ☐ Binding Corporate Rules (BCRs)
- ☐ Model Contract Clauses
- ☐ Privacy Shield
- ☐ Other

Does the company have data centers outside the US and/or EU?

- ☐ Yes
- ☐ No

Does the company have integrated, global or enterprise-wide human resources information systems (HRIS)?

- ☐ Yes
- ☐ No

Is personal data about employees located outside of the US or EU stored in the HRIS?

- ☐ Yes
- ☐ No

Does the company have policies that are subject to approval by EU Works Councils?

- ☐ Yes
- ☐ No