zinfi™

GDPR Preparation Checklist

Ext.prc.001.02 | 05.05.2018

zinfi

Introduction

Organizations will need to be compliant with the GDPR by May 25, 2018. This regulation requires much more than simply updating policies, procedures and processes. It is an organization-wide responsibility that requires a high level of accountability and imposes sweeping changes in the way we manage personal data. If you haven't started yet, now is the time to put your GDPR readiness plan into action. To help, we have created this checklist to guide you and to track your progress toward full compliance.

GDPR Checklist

No	Issue	Tasks
1	**Corporate Governance**	
a	Storage of Records (Article 30)	Data controllers must maintain records of processing of the following: (a) the name and contact details of the controller and the data protection officer (if one is appointed); (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) transfers of personal data to a third country or an international organisation, including the name of the country or international organisation and, the documentation of the safeguards for the transfer (i.e. based on consent, necessary to perform a contract, public interest); (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures.
b	Data Protection Office (Article 37)	Establish whether the company is required to have a Data Protection Office i.e. where one of the following applies: (a) processing is carried out by a public body, except for courts; (b) core activities consist of monitoring operations which by virtue of their nature, scope or purposes require regular and systematic monitoring of data subjects on a large scale; or (c) core activities consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences.

		Even if the company is not required to have a Data Protection Officer, you may appoint a Data Protection Officer. Data Protection Officer contact details must be notified to the regulatory authority and published to the public.
c	Data Retention (Article 5)	Data can be retained only for as long as necessary for the purpose for which it was obtained. The company needs to determine how long data can be kept before it is either deleted or anonymized.
d	Privacy Impact Assessment ("PIA") (Article 35)	When a company implements new technologies which will or could result in a high risk to the rights and freedoms of individuals, the company must carry out a formal PIA. This is an exercise to determine what impact the technology and processing will have on individuals and to ensure that it adheres to all aspects of GDPR.
e	Employee training (Article 5)	Employees who handle personal data of other employees or customers must receive training in order to ensure that they handle it in accordance with GDPR. The company should keep a record of training and provide regular updates and refresher training.
f	Policies and procedures (Article 5)	In order to ensure that a company has considered its privacy obligations and adheres to the six data protection principles related to the processing of personal data as outlined in Article 5, the company must develop and implement data protection policies. There is no set format for these policies, and exact policies will be different for different companies, depending on the kind of data they process and why. Here is a list of common policy topics: • General Data Protection Policy • Data Subject Access Rights and Procedures • Data Retention Policy • Data Breach Escalation and Checklist • Employee Privacy Policy and Notice • Policy for Processing Customer Data • Guidance on Privacy Notices

2	**Privacy notices (Articles 12-14)**	
a	Are privacy notices given at the correct time to data subjects?	Notices must be given at the time that the data is obtained from the data subject, or if the data was received from a third party, within a reasonable period after obtaining the data but at the latest within one month.
b	Do privacy notices contain all of the required information?	The required information includes: (a) the identity and the contact details of the controller and data protection officer (where applicable); (b) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, including the legitimate interests pursued by the controller; (c) the recipients or categories of recipients of the personal data, if any; (d) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and how the transfer ensure adequacy of protection (i.e. which of the approved transfer mechanisms are used); (e) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (f) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (g) where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (h) the right to lodge a complaint with a supervisory authority; (i) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (j) the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

C	Language / form of privacy notices	Is the language concise, transparent, intelligible and in an easily accessible form, using clear and plain language in particular for information addressed to a child? Consider whether the notice is delivered in a format that is user-friendly (e.g., font size and amount of text delivered on handheld devices) and the manner of delivery (e.g., "just-in-time" notices as customers fill in a web form or request certain functionality, or layered notices so that individuals can do a quick read of key points or the follow-up in more detail if desired).
3	**Lawfulness of processing**	
a	Has the company established a legal basis for processing all the different (non-sensitive) personal data that it holds? (Article 6)	These are the grounds for processing lawfully: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
b	Has the company established a legal basis for processing all the special categories of personal data (previously known as sensitive personal data) that it holds? (Article 9)	The legal grounds are as follows: (a) the data subject has given explicit consent; (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law; (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

		(d) processing relates to personal data which are manifestly made public by the data subject; (e) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (f) processing is necessary for reasons of substantial public interest; (g) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services; (h) processing is 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 quality and safety of health care; (i) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
c	Where the grounds for processing is consent (Article 7)	(a) Was the consent freely given? (b) Is the consent presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language? (c) Can the company demonstrate that the data subject gave their consent? (d) Does the data subject have the ability to withdraw their consent?
d	Profiling (Article 22)	(a) Does the company carry out profiling on employees or customers? (b) If so, does this profiling result in making a decision about the individual which would have a significant legal effect or similar on that individual—e.g., refusal of credit or refusal of an interview? (c) If the answer to (b) is yes, has the company obtained the consent of the individuals to this profiling?
e	Children (Article 8)	Does the company process the personal data of children? If so, consider language of privacy notices and how valid parental consent will be obtained.

4	**Data Subject Rights**	
a	Data Subject Access Right (Article 15)	Does the company enable employees and customers to request their personal data processed by the company? Are there personnel trained to respond to requests within a one-month timeframe?
b	Does the company have the processes or technology to enable data subjects to exercise their rights? (Articles 16-21)	Summary of data subject rights: (a) Right to rectification of inaccurate data. (b) Right to erasure ("right to be forgotten")—where data is no longer necessary in relation to the purpose for which they were collected, the data subject withdraws consent, objects to the processing, data is processed unlawfully, for compliance with a law or the data concerns a child and was processed by a website. The company needs to be able to identify other data controllers to whom it has disclosed data to tell them that the individual wants to be forgotten (subject to cost and available technology). (c) Right to restriction of processing to verify accuracy of data, where processing is unlawful but the individual does not want erasure, the controller no longer needs the data but the individual requires the controller to keep the data for defense of legal claims or pending verification of whether the legitimate interests of the controller in processing override those of the individual. (d) Right to data portability – controllers have to give data subjects their data in a format which the individual can take to another controller. (e) Right to object where processing is based on public interests or legitimate interests or for direct marketing.
5	**Privacy by Design and Default (Article 25)**	
a	Privacy by Design	Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

b	Privacy by Default	The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
6	**Data processors and international transfers**	
a	Does the company use third-party data processors or group companies to process data on its behalf? (Article 28)	If so, there must be a written contract with each data processor which must include the minimum requirements from Article 28. The company must also ensure that it has received "sufficient guarantees" from its data processors that they can implement measures (technical and organizational) to meet the requirements of the GDPR. Before there are any approved codes of conduct or certifications that controllers can rely on, the company will need to make its own enquiries through due diligence processes and perform its own assessment about whether its processors are complying with GDPR.
b	Does the company, or does the company's processors, transfer data out of the European Economic Area (EEA)? (Articles 44-49)	If so, which of the approved transfer mechanisms are used? The approved transfer mechanisms are as follows: (a) A country which has a finding of adequacy from the European Commission. (b) If it is within the company group, there must be binding corporate rules in place. (c) Standard contractual clauses as approved by the European Commission. (d) If the transfer is to the US, on the basis of the Privacy Shield. (e) With the consent of the data subject. (f) The transfer is necessary to carry out a contract with the data subject. (g) The transfer is in the public interest. (h) The transfer is necessary to establish, exercise or defend legal rights. (i) The transfer is necessary to protect the vital interests of a person where the data subject is physically or legally incapable of giving consent.

7	**Security**	
a	Are security measures appropriate for the personal data (Article 32)?	Security has to be appropriate to the likely risks to individuals if data was lost, stolen or disclosed to unauthorized people. Organizations can take into account the state of art, costs and the nature, scope and context of processing in order to determine what is appropriate to the risks involved. Security covers organizational (i.e., people and processes) and technical measures. The following factors should be considered: • Pseudonymization • Encryption • Ensuring ongoing integrity, confidentiality, availability and resiliency • The ability to restore in a timely manner • Processes for testing security
8	**Breach notification**	
a	Mandatory notification (Article 33)	Does the company have procedures in place to enable it to report a breach to the regulator within 72 hours of becoming aware of it? The breach must be investigated, and details provided to the regulator about the nature of the breach, likely consequences and mitigations being taken to address it. This investigation may require assistance from processors, so operational processes should factor this in.
b	Notification to individuals affected (Article 34)	If the breach is likely to result in a high risk to the rights and freedoms of individuals, the company will need to notify the individuals affected. Note that if data is encrypted or otherwise unintelligible, then individuals will not need to be notified.

www.zinfi.com

Contact Us

AMERICAS

sales.noram@zinfitech.com
6200 Stoneridge Mall Road, Suite 300
Pleasanton, CA 94588
United States of America

EUROPE, MIDDLE EAST AND AFRICA

sales.emea@zinfitech.com
Davidson House
Forbury Square, Reading
RG1 3EU, United Kingdom

ASIA PACIFIC

sales.ap@zinfitech.com
3 Temasek Avenue
#21-00 Centennial Tower
Singapore 039190

Australia • China • Hong Kong • India • Indonesia • Japan • Korea • Romania • Singapore • UK • USA