VISTA INFOSEC®

TRUSTED ADVISORS, ASSURED COMPLIANCE™

GDPR Compliance Checklist 2022

W: www.vistainfosec.com | E: info@vistainfosec.com

US Tel: +1-415-513-5261 | UK Tel: +442081333131 | SG Tel: +65-3129-0397

IN Tel: +91 73045 57744 | DUBAI Tel: +971507323723

An ISO27001 Certified Company, CERT-IN Empanelled, PCI QSA, PCI QPA and PCI SSFA

USA. SINGAPORE. INDIA. UK. MIDDLE EAST. CANADA.

INDEX

OVERVIEW OF EU GDPR REGULATION 04-05

ACCOUNTABILITY & GOVERNANCE 06-27

LAWFUL PROCESSING OF DATA 20-21

PRIVACY BY DESIGN & DEFAULT 28-29

DATA SECURITY 28-31

PRIVACY NOTICE 32-41

DATA SUBJECT RIGHTS 40-85

BREACH NOTIFICATION 84-87

Next Step - GDPR Readiness 88-91

OVERVIEW OF EU GDPR REGULATION

General Data Protection Regulation (GDPR) is a global data privacy law established and enforced in the EU. It is a comprehensive law developed to protect and uphold the rights of EU Citizens. Organizations dealing with the personal data of citizens of the EU are required to comply with the requirements of GDPR. This brings in more transparency in the processing and securing of personal data while also ensuring citizens have control over their personal data. Complying with the requirements outlined in the GDPR can be a daunting task for organizations as the requirements outlined are largely detailed and extensive. So for the benefit of our readers and organizations looking to achieve GDPR Compliance we have shared a comprehensive GDPR Compliance Checklist for 2022. The following detailed checklist which is an excerpt from the GDPR requirements can help you understand the regulation and guide your business in taking the right steps to prioritize security and privacy of data. The document contains only the important requirements in the below-listed excerpt from the GDPR requirements that is essential to ensure compliance.

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE		
Article 5	Principles of Processing Personal Data	1. Controllers should ensure the personal data is processed lawfully, fairly and in a transparent manner concerning the data subject. 2. Collected for specified, explicit, and legitimate purposes should not further be processed in a manner that is incompatible with those purposes. 3. Ensuring data minimization in terms of processing adequately, relevant and limited to what is necessary for the purposes for which they are processed. 4. Ensure accuracy of data and where necessary, keep up to date with every reasonable step taken to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, erased, or rectified without delay. 5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE		
Article 5	Principles of Processing Personal Data	6. Personal data may be stored for longer periods so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes with appropriate implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject. **7. Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organizational measures.** **8. Controller shall be responsible for, and be able to demonstrate compliance to the principles of processing personal data.**
Article 35	Data Protection Impact Assessment	1. The controller shall prior to the processing carry out a data protection impact assessment to envisage processing operations on the protection of personal data considering the type of processing personal data using

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE

Article 35	Data Protection Impact Assessment	new technologies, and taking into account the nature, scope, context, and purposes of the processing, that may likely result in a high risk to the rights and freedoms of natural persons. 2. The assessment shall contain at least ■ Systematic description of the envisaged processing operations and the purposes of the processing, including, the legitimate interest pursued by the controller. ■ Assessment of the necessity and proportionality of the processing operations concerning the purposes. ■ Assessment of the risks to the rights and freedoms of data subjects. ■ Measure risk to address it, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE		
Article 35	Data Protection Impact Assessment	3. Compliance with approved codes of conduct as in Article 40 by the relevant controllers or processors should consider in assessing the impact of the processing operations performed in particular for the purposes of a data protection impact assessment. 4. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. 5. Where necessary the controller shall review to assess if the processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.
Article 37	Appointment of Data Protection Officer	1. Establish whether the company is required to have a DPO where one of the following applies ■ Processing is carried out by a public body, except for courts;

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE

Article 37	Appointment of Data Protection Officer	■ 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 ■ Core activities consist of processing a large scope of special categories of personal data and data relating to criminal convictions and offenses. 2. If the company is not required to have a DPO, you may appoint a voluntary DPO. 3. DPO contact details must be notified to the regulatory authority and published to the public.
Article 30	Record Keeping	1. The controller and the controller's representative, where applicable, shall maintain a record of processing activities under its responsibility and include the following information- ■ Name and contact details of the controller and, where applicable, the joint controller, the controller's representative, and the data protection officer.

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE

Article 30	Record Keeping	■ Purposes of the processing. ■ Description of the categories of data subjects and the categories of personal data. ■ Categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations. ■ Details of transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and the documentation of suitable safeguards. ■ Where possible, the envisaged time limits for erasure of the different categories of data. ■ Where possible, a general description of the technical and organizational security measures.

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE

Article 30	Record Keeping	2. The Processor or Processor representative where applicable shall maintain a record of all categories of processing activities carried out on behalf of a controller including- ■ Name and contact details of the processor or processors and of each controller on behalf of which the processor is acting and, where applicable, of the controller's or the processor's representative, and the data protection officer. ■ Categories of processing are carried out on behalf of each controller. ■ Where applicable details of transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, documentation of suitable safeguards. ■ General description of the technical and organizational security measures. 3. Records shall be in writing, including in electronic form.

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE		
Article 30	Record Keeping	4. Controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.
LAWFUL PROCESSING OF DATA		
Article 6	Establish legal basis and grounds on which data controller processes personal data.	1. The data subject has given consent to process personal data for one or more specific purposes. 2. Processing is necessary for the performance of a contract to which the data subject agreed or to take certain steps at the request of the data subject prior to entering into the contract. 3. Processing is necessary for compliance with a legal obligation to which the controller is subject. 4. Processing is necessary to protect the vital interests of the data subject or another natural person. 5. Processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller.

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE

Article 6	Establish legal basis and grounds on which data controller processes personal data.	6. Processing is necessary for 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, especially wherein the data subject is a child.
Article 7	Establish legal basis and grounds for processing through consent	1. Ensure to process personal data based on free consent 2. The consent presented should be clear and precise distinguishable from other matters, in an intelligible and easily accessible format using clear and plain language. 3. The data controller should be able to demonstrate that the data subject freely gave their consent. 4. The data subject is informed about their ability to withdraw their consent anytime they wish to do so.

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE		
Article 9	Establish legal basis and grounds on which data controller processes all special categories of personal data.	1. The Data Subject has given explicit consent. 2. Processing is necessary for carrying out the obligations and exercising specific rights of the controller or the data subject in the field of employment and social security and social protection law. 3. 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. 4. Processing relates to personal data that are made public by the data subject. 5. Processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts are acting in their judicial capacity. 6. Processing is necessary for reasons of substantial public interest. 7. Processing is necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, provision of health or social care, or treatment or management of health or social care systems and services.

IMPORTANT GDPR COMPLIANCE CHECKLIST

ACCOUNTABILITY & GOVERNANCE		
Article 9	Establish legal basis and grounds on which data controller processes all special categories of personal data.	8. 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. 9. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.
Article 22	Automated Decision Making & Profiling	1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects. 2. The Data Controller should get the consent of the individuals for profiling and automated decision making.

IMPORTANT GDPR COMPLIANCE CHECKLIST

PRIVACY BY DESIGN & DEFAULT		
Article 25	Privacy by Default	The controller shall implement appropriate technical and organizational measures to ensure by default, only personal data necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their procesxsing, 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.
DATA SECURITY		
Article 32	Security of Data Processing	1. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller, and the processor, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SECURITY

Article 32	Security of Data Processing	■ Pseudonymisation and encryption of personal data ■ Ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services ■ Measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident ■ Process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. 2. Adherence to an approved code of conduct as in Article 40 or an approved certification mechanism as in Article 42 may be used as an element by which to demonstrate compliance with the requirements. 3. Ensure that controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller unless he or she is required to do so by Union or Member State law.

IMPORTANT GDPR COMPLIANCE CHECKLIST

PRIVACY NOTICE		
Article 12	Language and communication in Privacy Notice	1. The language in the Privacy notice should be clear concise, transparent, intelligible and in an easily accessible form, using plain language in particular for information addressed to a child. 2. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 3. Where the data subject requests by electronic form mean, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. 4. The Privacy Notice should be delivered in a format that is user-friendly which means in readable font size and text easily visible, intelligible, and legible manner with a meaningful overview of the intended processing.

IMPORTANT GDPR COMPLIANCE CHECKLIST

PRIVACY NOTICE		
Article 12	Language and communication in Privacy Notice	5. Information provided under Articles 13 and 14 where the personal data is either collected by the data subject or third party and any communication and any actions taken under Articles 15 to 22 which is concerning the rights of data subjects and communication of data breach under Article 34 shall be provided free of charge. 6. In case the request from the data subject are manifestly unfounded or excessive, in particular, because of their repetitive character, the controller may either: ■ Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or ■ Refuse to act on the request. The Data controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

IMPORTANT GDPR COMPLIANCE CHECKLIST

PRIVACY NOTICE		
Article 13	Privacy Notice must be given in a timely manner to the data subject	The Privacy Notices must be given at the time the data is obtained from the data subject, or from a third party, but within a reasonable period after obtaining the data which is at the latest within one month.
Article 13	Privacy Notice must be given in a timely manner to the data subject	The information to be mentioned in the privacy notice should include ■ The identity and the contact details of the controller and data protection officer (where applicable) ■ Purposes of processing the personal data and the legal basis for the processing, including the legitimate interests pursued by the controller. ■ Recipients or categories of recipients of the personal data, if any. ■ Inform and provide details where the controller intends to transfer personal data to a third country or international organization. Also, provide details on how the transfer ensures the adequacy of protection (i.e. which of the approved transfer mechanisms are used).

IMPORTANT GDPR COMPLIANCE CHECKLIST

PRIVACY NOTICE

Article 13	Privacy Notice must be given in a timely manner to the data subject	■ Period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. ■ 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 the processing as well as the right to data portability. ■ 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. ■ Right to complain with a supervisory authority. ■ 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.

IMPORTANT GDPR COMPLIANCE CHECKLIST

PRIVACY NOTICE		
Article 13	Privacy Notice must be given in a timely manner to the data subject	■ Existence of automated decision-making, including profiling, meaningful information about the logic involved, and the significance and probable consequences of such processing for the data subject.
DATA SUBJECT RIGHTS		
Article 15 - 22		GDPR is about upholding the rights of data subjects and so the data controller must ensure having in place measures to comply with the rights of data subjects listed below.
Article 16	Right to Rectification	1. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. 2. Considering the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 17	Right to Erasure	1. The data subject shall have the right to the erasure of personal data concerning him/her without undue delay and the controller shall have the obligation to erase personal data without undue delay. 2. The grounds for obligation stands on- ■ When personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed. ■ The data subject withdraws consent on which the processing is based on the lawfulness (Article 6) and for special category data (Article 9) and now where there is no other legal ground for the processing. ■ The data subject objects to the processing and there are no overriding legitimate grounds for the processing. ■ Personal data has been unlawfully processed ■ Personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS		
Article 17	Right to Erasure	■ Personal data have been collected in relation to the offer of information society services as per Article 8
Article 18	Right to Restrict Processing	The data subject shall have the right to restriction of processing of data wherein- ■ If the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data the processing shall be restricted. ■ Processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead. ■ The controller no longer needs the personal data for the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims. ■ The data subject has objected to processing according to pending verification whether the Data Controller has legitimate grounds to override those of the data subject.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS		
Article 19	Right to Notification obligation regarding rectification, erasure, and restriction of processing personal data	1. The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17 & Ar-ticle 18. 2.The controller must also notify each recipient to whom the personal data have been disclosed unless this proves impossible or involves disproportionate effort. 3.The controller shall inform the data subject about those recipients if the data subject requests it.
Article 20	Right to Data Portability	1. Data subject shall have the right to receive the per-sonal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format. 2. The Data Subject has the right to data portability where the data subject shall have the right to have the personal data transmitted directly from one controller to another without hindrance from the controller, where technically feasible.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 21	Right to object	1. Data subject shall have the right to object the processing of his/her personal data at any time including profiling unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data sub-ject or for the establishment, exercise or defense of legal claims. 2. Data subject shall have the right to object at any time to processing of personal data concerning him/her where personal data is processed for direct marketing purposes including profiling. 3. The Controller must at the time of the communication with the data subject, shall explicitly bring to the attention of the data subject their right to object processing under Article 6 and shall be presented clearly and separately from any other information. 4. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise their right to object by automated means using technical specifications.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS		
Article 21	Right to object	5. Where personal data are processed for scientific or historical research purposes or statistical purposes as per Article 89, the data subject, on grounds relating to their particular situation shall have the right to object the processing of personal data concerning them unless the processing is necessary for reasons of public interest.
Article 22	Automated Individual Decision making including profiling	1. Data subjects have the right not to be subject to a de-cision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them. 2.In the case where the right to a decision on automat-ed processing cannot be exercised on the grounds of – ■ Necessary for entering into, or performance of, a contract between the data subject and a data con-troller. ■ Authorized by Union or Member State law to which the controller is subject. ■ Based on the data subject's explicit consent.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 22	Automated Individual Decision making including profiling	The data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express their point of view, and to contest the decision. 3. The decision of not exercising the right to automated processing by the data controller is not applicable for special category data as under Article 9 again unless – ■ Data subject had given explicit consent to the processing of personal data for one or more specified purposes, except where Union or Member State law provides that the prohibition. ■ Processing is necessary for reasons of substantial public interest, based on Union or Member State law. But with suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS		
Article 23	Restriction	1. Right to restriction of processing to verify accuracy of data, or where processing is unlawful but the data subject opposes the erasure of the personal data and rather requests the restriction of their use. 2. Right to restriction also applies wherein the controller may no longer need the data but the data subject requires the controller to keep the data for the defense of legal claims or pending verification of whether the legitimate interests of the controller in processing override those of the individual.
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS		
Article 44	Transfer of data to a third country or international organization	1. Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or an international organization shall take place only if, subject to provisions and ensure that the level of protection of data subject is guaranteed by this Regulation is not undermined. The transfer of personal data transfer to a third country or an international organization shall take place based on-

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS		
Article 44	Transfer of data to a third country or international organization	■ Transfer based on adequacy ■ Transfers subject to appropriate safeguards ■ Transfers based on binding corporate rules ■ Transfer or disclosure not authorized by Union Law ■ Derogation to the specific situation ■ International Corporation for the protection of personal data.
Article 45	Transfer on the basis of adequacy	1. Transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory, or specified sectors within that third country, or the international organization ensures an adequate level of protection. 2. Transfer of personal data to a third country or an international organization based on assessing the adequacy of the level of protection considering –

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 45	Transfer on the basis of adequacy	■ Rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security, and criminal law, and the access of public authorities to personal data. ■ Implementation of such legislation, data protection rules, professional rules, and security measures, including rules for the onward transfer of personal data to another third country or international organization which is complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred. ■ existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject to responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 45	Transfer on the basis of adequacy	■ International commitments to the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments and its participation in multilateral or regional systems, in particular in relation to the protection of personal data. 3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or more specified sectors within the third country, or an international organization ensures an adequate level of protection and the implementing act provides for a mechanism for a periodic review, at least every four years, taking into account all relevant developments in the third country or international organization. 4. Commission shall, on an ongoing basis, monitor developments in third countries and international organizations that could affect the adequacy level of protection.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS		
Article 45	Transfer on the basis of adequacy	5. Commission shall, where available information reveals, that third country, a territory or specified sectors within a third country, or an international organization no longer ensures an adequate level of protection to the extent necessary, repeal, amend or suspend the decision by means of implementing acts without retroactive effect. 6. Commission shall enter into consultations with the third country or international organization to remedy the situation giving rise to the decision made by means of implementing acts. 7. The decision taken to transfers personal data to the third country, a territory, or one or more specified sectors within that third country, or the international organization is without prejudice. 8. Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories, and specified sectors within third countries and international organizations that have or do not have an adequate level of protection. 9. Decisions adopted by the Commission shall remain in force until amended, replaced, or repealed by a Commission Decision.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS		
Article 46	Transfer Subject to appropriate safeguard	1. The Controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. 2. The appropriate safeguards provided for shall be without requiring any specific authorization from a supervisory authority, by- ■ Legally binding and enforceable instrument between public authorities or bodies ■ Binding corporate rules in accordance with Article 47 ■ Standard data protection clauses adopted by the Commission in accordance with the examination procedure as under Article 93 of Committee Procedures. ■ An approved code of conduct as under Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS		
Article 46	Transfer Subject to appropriate safeguard	3. If subject to authorization from the competent supervisory authority, the appropriate safeguards may also be provided for, in particular, by ■ Contractual clauses between the controller or processor and the controller, processor, or the recipient of the personal data in the third country or international organization. ■ Provisions to be included in the administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. ■ The supervisory authority shall apply the consistency mechanism as under Article 63. 4. Authorisations by a Member State or supervisory authority based on Joint Controller as under Article 26(2) shall remain valid until amended, replaced, or repealed, if necessary, by that supervisory authority. 5. Decisions adopted by the Commission based on the Article 26 Joint Controller shall remain in force until amended, replaced, or repealed, if necessary, by a Commission Decision adopted in accordance with Article 46 of Transfer Subject to appropriate safeguard.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 47	Binding Corporate Rules	1. Competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they- ■ Are legally binding and applies to and is enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees. ■ Expressly confer enforceable rights on data subjects concerning the processing of their personal data. ■ Fulfill the requirements by providing details as mentioned in the binding corporate rules. 2. Binding corporate rules shall specific details such as - ■ Structure and contact details of the group of undertakings, or group of enterprises engaged in joint economic activity and of each of its members. ■ Data transfers or set of transfers, including the categories of personal data, type of processing and its purposes, the type of data subjects affected, and the identification of the third country or countries in question

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 47	Binding Corporate Rules	■ Legally binding nature, both internally and externally ■ Application of the GDPR principles, including purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, the legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements concerning the onward transfers to bodies not bound by the binding corporate rules. ■ Rights of data subjects regarding the processing and exercising rights, including the right not to be subject to automated processing, including profiling, right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and obtain redress and, where appropriate, compensation for a breach of the binding corporate rules.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 47	Binding Corporate Rules	■ Acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union. That said, the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage. ■ How the information on the binding corporate rules, in particular on the provisions Application of the GDPR principles, Rights of data subjects, Acceptance of liability for any breaches is provided to the data subjects in addition to Articles 13 which is information to be provided where personal data are collected from the data subject 14 which is Information to be provided where personal data have not been obtained from the data subject. ■ Tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 47	Binding Corporate Rules	■ Complaint procedures ■ Mechanisms for ensuring the verification of compliance with the binding corporate rules mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. ■ Mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority. ■ Cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures. ■ Mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 47	Binding Corporate Rules	■ Appropriate data protection training to personnel having permanent or regular access to personal data. 3. Commission may specify the format and procedures for the exchange of information between controllers, processors, and supervisory authorities for binding corporate rules. 4. The implementing acts shall be adopted in accordance with the examination procedure set out in Article 93
Article 48	Transfers or disclosures not authorized by Union law	1. Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 49	Derogations for specific situations	1. In the absence of an adequacy decision or of appropriate safeguards including binding corporate rules as under Article 45, Article 46, Article 47, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only on one of the following conditions- ■ The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards. ■ The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request. ■ The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person. ■ The transfer is necessary for important reasons of public interest.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 49	Derogations for specific situations	■ The transfer is necessary for the establishment, exercise, or defense of legal claims. ■ The transfer is necessary to protect the interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent. ■ The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. ■ The transfer could not be based on a provision in adequacy decision or appropriate safeguards including binding corporate rules as under Article 45, Article 46, Article 47, and none of the derogations for a specific situation, the transfer to a third country or an international organization may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, and necessary for the purposes of compelling legitimate interests by

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS

Article 49	Derogations for specific situations	the controller that does not override the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has based on that assessment provided suitable safeguards concerning the protection of personal data. ■ The controller shall inform the supervisory authority of the transfer and also provide the information referred to in Articles 13 and 14, to the data subject of the transfer and on the compelling legitimate interests pursued. 2. Transfer shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. 3. In the case where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients. 4. Transfer of data based on public interest shall be recognized in Union law or in the law of the Member State to which the controller is subject.

IMPORTANT GDPR COMPLIANCE CHECKLIST

DATA SUBJECT RIGHTS		
Article 49	Derogations for specific situations	5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organization. Further, this provision shall be notified to the commission. 6. Controller or processor shall document the assessment and the suitable safeguards in accordance with Article 30 of Records of processing activities.
BREACH NOTIFICATION		
Article 33	Breach Notification to Supervisory Authority & Data subject	1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority. 2. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. 3. Processor shall notify the controller without undue delay after becoming aware of a personal data breach.

IMPORTANT GDPR COMPLIANCE CHECKLIST

BREACH NOTIFICATION

Article 33	Breach Notification to Supervisory Authority & Data subject	4. Notification must include information that- ■ Describe the nature of the personal data breach including where possible, the categories and the approximate number of data subjects concerned and the categories and the approximate number of personal data records concerned. ■ Communicate the name and contact details of the data protection officer or other contact points where more information can be obtained. ■ Describe the likely consequences of the personal data breach. ■ Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. 5. Where, and as far as if not possible to provide the information at the notifying the breach, the information may be provided in phases without undue further delay. 6. Controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects, and the remedial action is taken.

Next Step - GDPR Readiness

Moving forward your organizations should take into account the following steps to ensure GDPR Compliance readiness before conducting the final audit.

Data Classification

Identify and Determine the kind of data that falls in scope of GDPR. Thereafter what sensitive or personal data needs to be protected which also includes keeping a track of who has access, to those data.

Awareness Training

Educate employees about the regulation and its requirements. Make them aware of their key responsibilities and consequences of not complying.

Governance

Orgainzation must determine whether they need to appoint a Data Protection Officer (DPO) and also define roles and responsibilities in terms of identifying who would be in charge of managing GDPR.

Next Step - GDPR Readiness

Moving forward your organizations should take into account the following steps to ensure GDPR Compliance readiness before conducting the final audit.

Integrate Security & Privacy Solution

Implement and integrate security, privacy by design and default in the organizations systems and processes. Integrate software that aids in the compliance process.

Policy & Process Implementation

Establish policies, procedures and processes that aids the security and privacy of data and helps in the compliance process.

Review & Monitor

Review the implemented policies, procedures and processes and ensure that the organization has prioritized security and privacy in its overall processes.

ACTIONABLE STEPS TO ACHIEVE GDPR COMPLIANCE

REGISTER FOR FREE ONE SESSION OF COMPLIANCE CONSULTATION

https://www.vistainfosec.com/book-free-compliance-consultation/

CONTACT US

US Tel: +1-415-513-5261 | UK Tel: +442081333131
SG Tel: +65-3129-0397 | IN Tel: +91 73045 57744
DUBAI Tel: +971507323723

www.vistainfosec.com

info@vistainfosec.com

FOLLOW US

ON OUR SOCIAL NETWORKS