The General Data Protection Regulation (GDPR) is a comprehensive data protection law that was enacted by the European Union (EU) in May 2018. Its primary purpose is to protect the privacy and personal data of individuals within the EU and the European Economic Area (EEA). Here's an overview:

### What is GDPR?

GDPR establishes strict guidelines for how organizations collect, store, process, and share personal data of individuals in the EU. It aims to give people more control over their personal data and to create a unified legal framework for data protection across the EU.

### How GDPR Works

* **Data Protection Principles**: GDPR outlines key principles that organizations must follow, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.
* **Consent**: Organizations must obtain clear and explicit consent from individuals before collecting their personal data. The consent must be freely given, specific, informed, and unambiguous.
* **Rights of Individuals**: GDPR grants individuals several rights, including the right to access their data, the right to rectification, the right to erasure (also known as the right to be forgotten), the right to restrict processing, the right to data portability, and the right to object to certain data processing activities.
* **Data Breach Notifications**: In case of a data breach, organizations must notify the relevant data protection authority within 72 hours and inform the affected individuals if the breach poses a high risk to their rights and freedoms.
* **Data Protection Officers (DPO)**: Some organizations are required to appoint a Data Protection Officer to oversee GDPR compliance and act as a point of contact for data protection authorities and individuals.
* **Accountability and Documentation**: Organizations must demonstrate compliance with GDPR through proper documentation, risk assessments, and, in some cases, conducting Data Protection Impact Assessments (DPIAs) for high-risk processing activities.
* **Penalties**: Non-compliance with GDPR can result in significant fines, up to €20 million or 4% of the global annual turnover of the preceding financial year, whichever is higher.

### Where GDPR Needs to Be Implemented

* **Within the EU/EEA**: Any organization that processes the personal data of individuals within the EU/EEA must comply with GDPR, regardless of where the organization is based.
* **Outside the EU/EEA**: GDPR also applies to organizations outside the EU/EEA if they offer goods or services to individuals in the EU/EEA or monitor the behavior of individuals within the EU/EEA.

### When GDPR Is Required

GDPR is required when an organization processes personal data that could directly or indirectly identify an individual, such as names, email addresses, IP addresses, location data, health information, and more. Organizations across various sectors, including finance, healthcare, e-commerce, and social media, must adhere to GDPR if they handle data of EU/EEA residents.

In your case, performing a GDPR security audit involves ensuring that the company adheres to these regulations, especially regarding the processing of Personally Identifiable Information (PII) and Special Categories of Personal Data (SPI).

**How can I performed that GDPR Security audit?**

Performing a GDPR security audit that involves checking for Personally Identifiable Information (PII) and Special Categories of Personal Data (SPI) requires a structured approach. Here's a step-by-step guide:

**1. Understand the Scope of the Audit**

* **Identify Data Types:** Determine the types of PII and SPI the company processes. PII includes names, addresses, contact information, and identification numbers, while SPI includes data on race, religion, health, sexual orientation, etc.
* **Identify Systems and Processes:** List all systems, databases, and processes where PII and SPI are stored, processed, or transferred.

**2. Review Data Handling Practices**

* **Data Collection:** Check how the company collects PII and SPI. Ensure data minimization principles are followed, meaning only necessary data is collected.
* **Data Storage:** Evaluate how and where PII and SPI are stored. Ensure encryption, access controls, and secure storage practices are in place.
* **Data Processing:** Examine how PII and SPI are processed, ensuring that processing activities are lawful, fair, and transparent.
* **Data Transfer:** Review data transfer processes, particularly cross-border transfers, to ensure they comply with GDPR requirements (e.g., Standard Contractual Clauses, Adequacy Decisions).

**3. Assess Legal Compliance**

* **Lawful Basis for Processing:** Verify that there is a lawful basis for processing PII and SPI (e.g., consent, contract, legal obligation).
* **Data Subject Rights:** Ensure mechanisms are in place for individuals to exercise their rights (e.g., access, rectification, deletion, portability).
* **Privacy Notices:** Review privacy notices to ensure they are clear, comprehensive, and accessible.

**4. Check for Data Breach Preparedness**

* **Incident Response Plan:** Assess the company's data breach response plan, ensuring it includes detection, containment, investigation, and notification procedures.
* **Data Breach Notification:** Verify that there is a process for notifying the supervisory authority and affected individuals within the required timeframe (72 hours for the authority).

**5. Evaluate Security Measures**

* **Access Controls:** Ensure that access to PII and SPI is restricted to authorized personnel only.
* **Encryption and Anonymization:** Check if PII and SPI are encrypted at rest and in transit and whether anonymization or pseudonymization techniques are applied where appropriate.
* **Data Retention and Deletion:** Ensure that PII and SPI are retained only as long as necessary and that deletion procedures are in place and followed.

**6. Documentation and Reporting**

* **Maintain Records:** Ensure that records of processing activities (ROPA) are maintained as required by Article 30 of the GDPR.
* **Audit Report:** Compile a report detailing findings, including any non-compliance issues and recommendations for remediation.

**7. Remediation and Follow-Up**

* **Address Findings:** Work with the company to address any gaps or non-compliance issues identified during the audit.
* **Follow-Up Audit:** Schedule follow-up audits to ensure that corrective actions have been implemented and sustained.

This approach will help you thoroughly assess the company's compliance with GDPR requirements regarding PII and SPI and provide actionable insights to improve their data protection practices.

**How do I perform the audit? what will be the steps?**

Performing a GDPR security audit, particularly focused on PII and SPI, involves several key steps. Here's a detailed process you can follow:

**1. Planning and Preparation**

* **Define Audit Objectives and Scope:**
  + **Objective:** Ensure compliance with GDPR regarding PII and SPI.
  + **Scope:** Determine which systems, processes, departments, and data types will be included in the audit.
* **Identify Stakeholders:**
  + Include data protection officers, IT staff, legal teams, and department heads involved in data processing.
* **Gather Documentation:**
  + Obtain relevant policies, procedures, data flow diagrams, and records of processing activities (ROPA).

**2. Data Inventory and Mapping**

* **Create a Data Inventory:**
  + List all the PII and SPI the company processes, including where and how the data is stored, processed, and transmitted.
* **Data Flow Mapping:**
  + Map out the flow of PII and SPI within the organization, including how it enters, moves through, and exits the organization.
* **Identify Processing Activities:**
  + Document all activities involving PII and SPI, including collection, storage, access, sharing, and deletion.

**3. Review Policies and Procedures**

* **Examine Data Protection Policies:**
  + Ensure the organization has robust data protection policies that align with GDPR requirements.
* **Assess Data Handling Procedures:**
  + Review how PII and SPI are handled at each stage of their lifecycle (collection, processing, storage, transfer, and disposal).
* **Evaluate Consent Mechanisms:**
  + Check if valid consent is obtained for processing PII and SPI where required, and if the organization can demonstrate this consent.
* **Review Third-Party Agreements:**
  + Ensure contracts with third-party processors include GDPR-compliant data protection clauses.

**4. Conduct Interviews and Assessments**

* **Interview Key Personnel:**
  + Speak with those involved in data processing to understand day-to-day practices and identify potential risks.
* **Assess IT Systems and Security Controls:**
  + Perform a technical assessment of systems that store or process PII and SPI, focusing on encryption, access controls, and data transfer security.
* **Check Compliance with Data Subject Rights:**
  + Test the organization’s ability to respond to data subject requests (e.g., access, rectification, erasure, and portability requests).
* **Evaluate Breach Detection and Response:**
  + Review incident response procedures to ensure timely detection, reporting, and response to data breaches involving PII and SPI.

**5. Analyze and Document Findings**

* **Identify Compliance Gaps:**
  + Compare current practices with GDPR requirements to identify any gaps or areas of non-compliance.
* **Evaluate Risk Levels:**
  + Assess the potential risks associated with any identified gaps, considering the likelihood and impact of a data breach or GDPR violation.
* **Document Findings:**
  + Compile your findings in a detailed audit report, including evidence, identified gaps, risk assessments, and recommendations.

**6. Provide Recommendations**

* **Develop a Remediation Plan:**
  + Provide actionable recommendations to address any gaps or weaknesses. Prioritize based on risk levels and GDPR requirements.
* **Suggest Improvements:**
  + Offer guidance on enhancing data protection measures, such as implementing stronger encryption, improving access controls, or refining data retention policies.
* **Training and Awareness:**
  + Recommend staff training on GDPR compliance and data protection best practices.

**7. Report and Follow-Up**

* **Present Audit Report:**
  + Share the audit report with senior management and relevant stakeholders, highlighting key findings and recommendations.
* **Monitor Remediation Efforts:**
  + Track the implementation of recommended actions and improvements.
* **Schedule Follow-Up Audits:**
  + Plan for follow-up audits to ensure continued compliance and effectiveness of corrective actions.

By following these steps, you'll be able to conduct a thorough GDPR security audit focused on PII and SPI, ensuring the company’s practices align with regulatory requirements.

# GDPR Compliance Checklist

We all know that compliance with the EU General Data Protection Regulation (GDPR) is essential for your company. We also know that non compliance is not an option. But how do you check whether you have done enough as a company? This is where our 12-step checklist can be handy for you. This can go a long way in helping you check and ascertain whether you are compliant with GDPR and have fulfilled the key requirements. This checklist can be applicable for data controllers and data processors.

## Step One - Data Inventory

Data inventory means you have created a map or view of all the personal data elements that your company processes i.e., what personal data and sensitive data you collect, what you process, where does it go, who is it shared with and how is a protected. Look at it, like inventory in a manufacturing unit, that is stock of what all is existing in a company. And here, since it's about data, we call it data inventory.  
  
If you've created a data inventory, sometimes also called Records of Processing Activity (ROPA) by some people, because that's how GDPR defines it in Article 30, you have taken one step forward towards compliance with EU GDDPR.

## Step Two - Data Expiration

In EU GDPR, you cannot keep personal data any longer than it is necessary. Infect, it is the same in UK GDPR or Data Protection Act. That means after the data has completed the purpose of processing, it must be deleted. For example, if I had subscribed to your newsletter, you have the right to keep my data. But if I have unsubscribed from the newsletter, you have no reason to keep data forever. And how long you should keep your data is a business decision plus a legal decision. Now you and your company need to have an approach on how long you keep the data. And when you expire it once a customer is no longer your active client.

If you have this approach, second item tick that is you have a data expiration or data retention or data deletion approach. Of course, I know it is challenging, because in the modern world, there is a soft, delete, hard delete and so many possibilities. But data exploration approach is a must for both structured and unstructured data that your company has.

## Step Three - Collect Consent

The third thing is consent. This means when you collect consent from individuals (or data subjects in legal terms) whose personal data you collect and process. And, you tell them what is it for? You don't bundle it. And you explain it in a simple and plain language while allowing them to withdraw their consent. How do you do it? And what do I mean by bundled? I mean, if I'm subscribing to your newsletter, that is one purpose. But if I subscribe to your event, then it's another purpose. So when I'm subscribing for an event, and you start sending the newsletter that is a strict no because it's a bundled consent. You can always ask me if I want to receive newsletter i.e., ask consent.  
  
If you've asked that and are allowing for the ability for an individual to withdraw his or her consent, that's a third tick i.e., one more step forward with your GDPR compliance.

### Step Four - Individual Rights

Individuals (data subjects in legal terms) that is people (may be your employees may be your customer, maybe your prospect maybe your supplier) whose personal data you process, have the rights to ask you for right to information, right to access, right to deletion and so on. For this your company must implement a process such that individuals can exercise their privacy rights. Privacy rights are also known as Data Subject Rights (DSRs), or simply Data Subject Access Rights (DSARs).  
  
If you have put in a process wherein individuals can exercise their privacy rights and you can answer those rights within 30 days, you have done  a good job. This means the fourth item that is individual rights is tick in the box and a step forward towards GDPR compliance.

### Step Five - Secure Data Transfers

In the modern worlds data flows. And in data economy, data also travels across countries. And, you need to make sure that the personal data that is being transferred is transferred in an adequate manner with adequate security with adequate controls. This means you have put in technical controls (i.e., implement data security measures), and organizational controls (i.e., implement data governance measures) for situations in which data is travelling outside of your company. You also put in contractual controls i.e.,  you sign a contract when you work with a third party. For example, when you work with a data processor, you add the necessary elements around processing in a Data Processing Agreement (DPA), or you use the Standard Contractual Clauses, or whatever is needed.  
  
If you have made sure that the personal data transfers in your company are adequately protected with adequate safeguards, you have done well to have the fifth item tick and move forward with GDPR compliance.

### Step Six - Ensure Transparency

Transparency means that you (as a data controller) always inform individuals (data subjects in legal terms) about collection and processing of personal data. This applies to collection and processing of customer data as well as employee data (and even personal data of supplier personnel). This includes telling them about: what personal data you collect, why you collect data,  what you do with it, who do you share it with, how can they exercise their rights, and so on... How do you do it? You do it through a privacy notice or a privacy statement. Normally, you provide a privacy notice whenever a screen is collecting personal data by showing in a link to the privacy notice. And, you also put in a privacy notice on your website.  
  
I you have done that, along with a cookie notice, and any other privacy notice at the time of collection of data, that's the sixth item that is transparency is ticked and you have moved a step closer to GDPR compliance.

### Step Seven - Awareness & Training

The seventh item or step is awareness and training. This means you have trained all your staff that processes personal data (or deals with personal data) to protect personal at all times. Legally you must train all relevant staff and also make aware about privacy,  personal data processing, and what you expect from them in terms of protecting personal data. While awareness would be ongoing, you must train your staff regularly. We recommend to train your staff at least once a year. In fact, we recommend to create department specific trainings with scenarios specific to each department.  
  
If you have done that, that is you have made the staff aware and trained them on privacy matters, a seven item is ticked and you have moved one more step closer to being GDPR compliance.

### Step Eight - Data Breach

Your data security team will do all the things that are necessary to protect data. But some times unintended, unauthorized access to personal data will happen. That is what we call a personal data breach. If that happens, how will you handle it? Who will detect it? How will you monitor it? And how will you remediate that situation? How do you manage personal data breaches? This is done by putting in place a personal data breach process. Once you have established the process, have you put in the capability to react and respond to these. in the EU GDPR, you will need to notify certain personal data breaches to authorities within 72 hours. You may also need to notify individuals or data subjects.   
  
If you have done that, that is you have put in process to detect and manage personal data breaches, you have taken a step forward in becoming GDPR compliant.

### Step Nine - Data Protection Impact Assessment (DPIA)

When processing involves significant amount of risk to the individual's rights and freedoms, then you need to conduct what we call a Data Protection Impact Assessment (DPIA). You also conduct DPIA when processing is at a large scale. Thankfully, this is not to be carried out on each and every process but only where necessary.   
  
If you're put in a process for DPIA and have carried out that the DPIA on high risk processes and documented the data protection risks,  you have done well. So that is nine item ticked and you have moved forward with your GDPR compliance objective.

## Step Ten - Assign a Data Protection Officer (DPO), if needed

Data Protection Officer not everyone needs it, but you must check if your company needs it. Data Protection Officer means a person who's there to oversee the implementation monitoring and ongoing compliance with EU GDPR.  
  
Have you checked whether your company needs a data protection officer or not? And, have you appointed one if necessary. If you've done that, that's the tenth item ticked and you have moved forward with your GDPR compliance objective.

## Step Eleven - Establish Privacy Operations Team

While you will do these as a project one time activity, the question is how are these things being done on a continuous basis? How is your staff taking care of it? Is it really happening what you have put in the project? How will you keep compliance actions up to date?  
  
For large companies, you would have your own staff. This is what we call a privacy office or team. This becomes a privacy operations team that will take care of the ongoing day-to-day requirements, make sure the policy and processes are being followed, answer the ongoing queries and so on. This team will also be looking out on any new requirements that need to be complied with.

For small companies, this will be usually in the form of an external consultant like me, or a company like us. This means you hire a company like manage us who can put a person on a full or part time basis. This is also known as privacy as a service.  
  
If you have put in a privacy operations team (or a privacy team or put privacy expert) to take care of ongoing requirements, and advise the business and monitor the privacy compliance on an ongoing basis, you are one step forward towards GDPR compliance.

## Step Twelve - Document and Evidence Actions

If you do all the eleven items we talked about and you don't do this one, it all goes to zero because GDPR asks for accountability. In fact, all privacy laws ask for accountability. Accountability means you as a company are taking care of compliance with law and can demonstrate it. This means you document your actions and keep this documentation up to data for demonstration of evidence later. Your data protection policies are also a form of evidence that you have taken necessary action(s).  
  
For example, if you have made a decision, let's say about DPO, and you decided not to appoint a DPO. Imagine, five years later your company would have grown. And there happens an incident and the authorities ask why didn't you appoint a DPO? Two scenarios are possible. One, have you documented that decision? If you have, you can show five years ago, this decision was made, this was the situation, these were the people who decided, and that's how it was made. And then the authority would say it's time to review it. But if you're not able to demonstrate because you don't have any evidence (or you don't have the documentation), then it's negligence (or non compliance) because you can't prove it. Then, the risk of fine increases. So always, always, always document all privacy decisions that your company makes.

If you have put in a process to document all privacy decisions and maintain the evidence on an ongoing basis, you have done one more right things and you are one more step forward with GDPR compliance.

## ****GDPR Compliance Checklist in a summary****

We do understand that GDPR compliance is a complex topic and evaluating your company's personal data collection, processing and personal data protection goes beyond any checklist. But I always recommend to start simple (where this list helps) and go deep into details for each of these because the devil is in detail. And, this has helped me and many of my clients in getting into details in a structured manner. Now, I hope the same for you as well. So, whether your company is processing personal data as a data controller or data processor, GDPR compliance is a must. And, this GDPR compliance checklist provides you with a starting point to start reviewing your data collection and processing practices.   
  
Summary of the 12-step General Data Protection Regulation (GDPR) compliance is:

* You have an up to date data inventory or Records of Processing Activity (ROPA)
* You have created and implemented a data expiration approach
* You have collected consent in lawful manner
* You have implemented  a process for Individual Rights
* You secure data transfers with third party vendors
* You demonstrate transparency relation to collection of personal data
* You have ensured privacy awareness & training for staff
* You have a process to detect, manage and notify a data breach
* You have conducted Data Protection Impact Assessment (DPIA), where necessary
* You appointed a Data Protection Officer (DPO) if necessary
* You have a Privacy Operations Team that can help you remain compliant
* You keep documentation that can be used as evidence  
    
  Finally, remember that this is not a legal advice. For specific legal advice, you must consult a professional to provide advice for becoming GDPR compliant. We wish you success in your compliance journey and hope that you process data of your customers, employees and personnel of suppliers in accordance with applicable privacy laws.  
    
  Now, its time to go and check if you are compliant or non-compliant. And, if you want to achieve GDPR compliance, or for that matter compliance with any privacy law, contact us and we shall be happy to have a call with you to help you.