The GDPR Compliance Workbook for HR

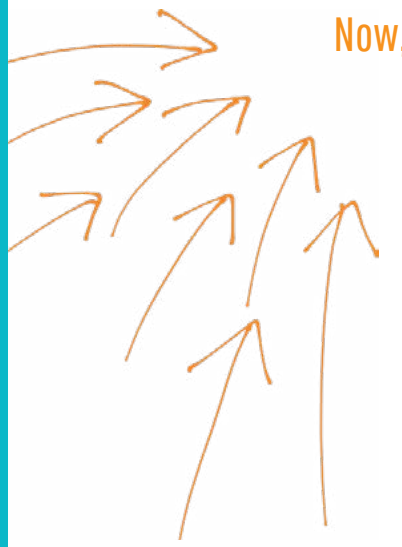
A practical guide for building an actionable compliance plan

peopledoc
BY ULTIMATE SOFTWARE

Introduction

If you're reading this, chances are you already know the GDPR has some major implications for HR compliance. But what you may not know is the GDPR isn't the big, bad wolf everyone makes it out to be. In fact, the GDPR presents the perfect opportunity for HR to re-evaluate their processes, showcase their dedication to security and transparency, and get a solid handle on all the employee data they manage.

Of course, these benefits don't change the fact that GDPR preparation takes time and work. That's why we put together this book. It will guide you through the right steps to ensure compliance so you can **stop spending time deciphering the rules and start taking action**. Each section is designed to get you started on your compliance journey by thinking through the HR processes, policies and practices that may need review and revision.



Now, let's get to work!

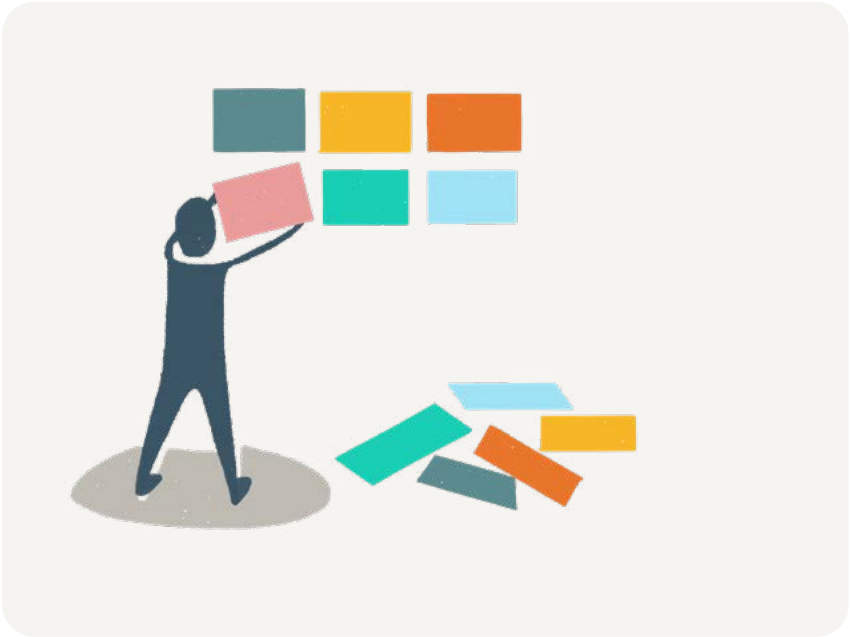
Psst!

This workbook is designed to help you start planning your approach to GDPR compliance. The templates and checklists are not intended to be comprehensive and will likely need to be adapted to your organization's unique circumstances.

Keep in mind, this workbook is not endorsed by a governing body nor is it a replacement for legal advice. The content has been informed by our experience working with clients addressing GDPR compliance and our own experience meeting GDPR requirements as both a data controller and processor.

Step 1: Build your task force

Your first task will be to assess all employee data across your organization—what data exists and where. But first, you need the right team. Your organization likely has an overall initiative for GDPR compliance, but it's HR's responsibility to make sure employee data is managed appropriately. HR can own this by forming a sub-committee with the specific task of protecting employees' private data. Start by recruiting representatives from HR, Legal, IT, Security and, if applicable, Governance, Risk and Compliance.



For an effective committee, be sure to:

- [ ] **Meet with department heads to determine the right committee members**
- [ ] **Identify those passionate about data privacy and encourage them to get involved**
- [ ] **Hold regular meetings with clearly-defined tasks**
- [ ] **Outline specific owners and due dates for each task**

GDPR Compliance Committee

Start by listing those who have a stake in employee data privacy. Down the line, you may find that you'll need to work more closely with some departments than others.

Department	Name	Title

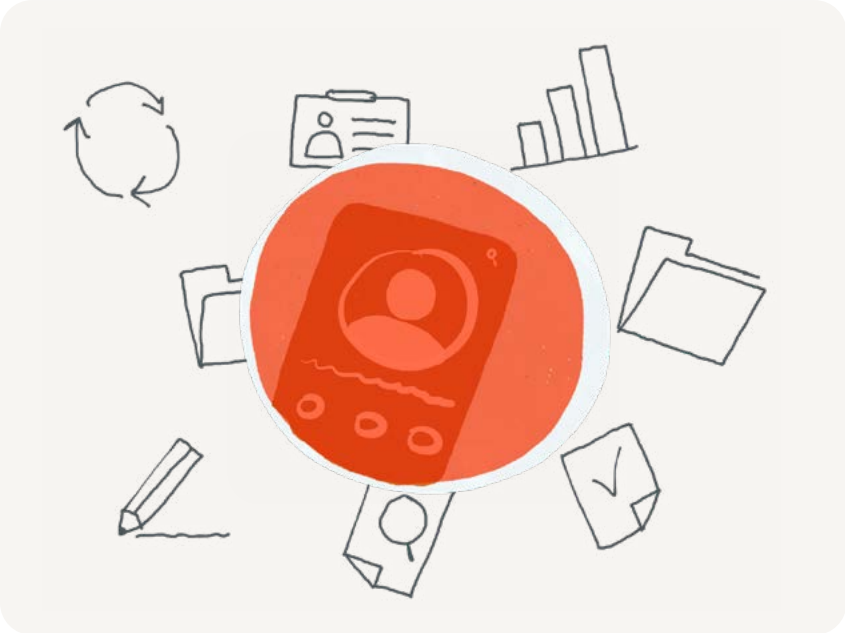
This committee will meet every: _____ **until** _____.

Step 2: Review and audit all personal data

To fully comply with GDPR, HR needs to inventory all the employee data it manages, especially personal data, such as birth dates, social security numbers, passport numbers, etc. This includes data on current employees as well as past employees, applicants, and any third party individuals (such as your employees' spouse or children).

In addition to the different types of employee data your team manages, you must also think about all the places this data lives. This can include your HRIS, performance management system, ATS, Excel sheets, and any filing cabinets or loose folders, if your organization has yet to go digital.

If you find that employee data is spread across multiple systems (or multiple offices), consider centralizing all data in one place. Maintaining data in a single system makes it easier to manage not only GDPR compliance, but HR compliance across the board.



Employee Data Assessment

The GDPR is based on the principle of minimization, which states that only data with a specific purpose should be collected. If it's not used regularly for day-to-day HR management, you're best off *not* requesting it. With that in mind, for each piece of personal data you will want to document the following information:

Data type:	
Data location:	
What's the specific purpose for this data?	
What's the legal basis for requesting this data?	
Do we still need this data?	
Has the individual been informed that this data is being processed?	
How often do we review this data for accuracy?	
What's our process for purging unnecessary data?	

Step 3: Assess who has access to data

Part of GDPR compliance is ensuring secure access to employee data. You will want to take stock of which individuals and roles have access to which types of employee data. This step should be taken for those within your organization (i.e., members of your HR or legal team) and for external parties (i.e., your payroll provider or HRIS vendor).

For internal employees, be sure the right individuals and roles have the appropriate level of access. Additionally, be sure to have a process in place for updating access as roles change.

The chart below can help you track who can access which types of data.

Employee Data Access

Title or role	Allow access to	Remove access to

Third-party access

For external businesses or subcontractors, consider which entities need access to employee data and how they plan to use that data. Under GDPR, an organization is held liable for the security of the employee data processed by third-party vendors or subcontractors. So, you'll want to be familiar with each subcontractor's security practices and be sure they comply with GDPR. Specifically, you want to understand their methods for securing employee data, especially as it's transferred across countries. For guidance, consult your local Data Protection Authority's Privacy Impact Assessment (PIA) or Data Protection Impact Assessment (DPIA) guidelines.

The most secure way to share employee data with both internal and external parties is electronically, using a system that lets you grant the right controls and security.

PeopleDoc's HR Service Delivery Platform allows only employees with the proper rights and roles to access documents, employee requests and forms, which can all include personal data.

Step 4: Review and update all privacy policies

The GDPR defines new rights for employees, such as the Right to Access and Right to Be Forgotten. Not only does HR need to uphold these rights, they must also formalize and clearly spell out these rights for employees under the GDPR's strengthened transparency requirements. To come into compliance, you may need to update or change your existing privacy notices. As you review them, use the checklist below to ensure each one covers all required points.

When assessing whether you're allowed to collect certain employee data, start from a legal or contractual requirement. You can use consent in certain instances, but relying on another a legal basis is preferred.

Privacy Notice Checklist:

- ☐ List which categories of data HR can collect
- ☐ Explain how HR will use that data and how long it will be stored
- ☐ When there's a legal basis for data collection, formally notify employees of the justification for collecting their data
- ☐ Indicate whether data will be transferred to other countries
- ☐ Inform individuals of their personal data rights (e.g., Right to Access, Right to Data Portability, etc.)
- ☐ Outline your organization's data protection responsibilities and the measures you take to ensure data security
- ☐ Use clear, concise and plain language

Step 5: Review and update all HR processes

Many of the individual rights under GDPR require new processes. HR will have to be prepared to respond to employee requests to view, modify or delete their personal data. For example, employees have the right to see all their data on file and, should they ask to view it, HR must turn around their request within 30 days, free-of-charge.

Along with new processes, it's a good idea to review and update all existing process that involve collecting and processing employee data (e.g., onboarding, employee transfers, or tuition reimbursement). The minimization principle comes into play here, too. As you think through each process, ask yourself, "*What is the least amount of data I need to complete this process?*" Your HR processes should be revised to collect only the data necessary for the task at hand.

On the next page, jot down how you plan to respond to some of the most likely scenarios under the GDPR.

Organizations must inform individuals of their personal data rights under the GDPR. The PeopleDoc HR Service Delivery Platform makes it easy to collect acknowledgments or signatures, reducing back-and-forth with employees.

Process preparation

How will we grant employees access to their data?

What will we do when an employee requests to correct their personal data?

Under what conditions can an employee request their data be deleted?

Under what conditions does HR need employee consent to process data?

Step 6: Prepare for the possibility of a data breach

A security breach is often an unexpected and stressful event, so it's important to have a well-documented process ahead of time, should you ever need it. Keep in mind that if an individual's information is compromised, the GDPR requires you to report the breach to the appropriate Data Protection Authority within 72 hours of discovery. And, you must notify any affected individuals without undue delay.

Work with your IT and Security teams to ensure you assign someone responsible for (1) investigating, (2) containing, (3) documenting and (4) reporting any breaches. Keep in mind, even in cases where you don't need to notify the Data Protection Authority, you still must retain a record of all data breaches.

Breach Documentation

Be sure any breaches are documented and include:

- **Details of the breach**
- **Impact of the breach**
- **Actions taken to remediate the breach**

Your subcontractors are also responsible for informing your organization in the event of a breach. Be sure to connect with them to ensure they have an appropriate data breach response plan in place.

Tip!

The best way to prepare for a potential data incident? Role play will illuminate the holes in your process. Reach out to all geographic locations and go through the steps as if it were real. Be sure to identify who's in charge of each responsibility, including notifying the affected individuals and communicating the incident internally.

Step 7: Determine whether you need a DPO

Certain types of employers are required to appoint a Data Protection Officer (DPO) under the GDPR. The DPO is charged with ensuring GDPR compliance and protecting personal data across the organization. You likely need a DPO if processing personal data is part of your company's core service or product (e.g., PeopleDoc is required to have a DPO because we process HR data for both our employees and clients).

If you *don't* need to hire a DPO, ensure you have a clear chain of command for all security and data management processes. If you *do* need to hire one, there are a few things to think about as you define the roles and responsibilities of the DPO.

Considerations for a DPO

- **Determine whether you can recruit someone from your existing headcount to serve as DPO (The DPO can fulfill other tasks as long as they're not in conflict with their data protection duties).**
- **Decide which department the DPO role will sit in (i.e., Legal, IT, Information Security or Data Governance)**
- **Consider whether you should hire a third party to fulfill the role of DPO**

Step 8: Inform and train employees

GDPR compliance requires cooperation from all employees, so it's important that everyone is versed in the latest compliance practices and knows who to contact if they suspect a breach. HR is responsible for incorporating compliance education into every new-hire's training and planning annual refresher training for all employees.

Employee compliance training checklist:

- [ ] **Communicate updated privacy policies and data processing notices to all employees**
- [ ] **Update employees on their data subject rights**
- [ ] **Train employees on reporting and escalating a breach**
- [ ] **Provide, at a minimum, annual training on security best practices**
- [ ] **Regularly refresh all communication and trainings**

Test your knowledge

How much do you know about the GDPR? See if you can correctly complete the following statements (find the answers on the next page!)

1. The fine for non-compliance can be up to ___ % of your organization's annual global revenue.

2. To cover all bases, HR needs a _____ _____ when collecting employee data.

3. The principle of _____ ensures HR collects only the data necessary for the task at hand.

4. In the event of a data breach, an organization must contact the local DPA within ___ hours of becoming aware of the incident.

5. The right to _____ _____ means employees can request a copy of the data concerning them.

6. Part of GDPR compliance is securing _____ to employee data.

7. If there's employee data on file that you don't need, you should _____ it.

8. GDPR compliance is _____'s job.

Extra credit

This workbook points you in the right direction for getting started with GDPR compliance, but to better understand what the GDPR means for HR, check out some of our in-depth resources.

Ultimate Guide

HR and the GDPR
Learn the key changes for HR, understand the benefits of GDPR and debunk the myths.

READ NOW

Checklist

GDPR for HR: The Ultimate Compliance Checklist
Tackle compliance with this 8-step framework.

START NOW

Case Study

GDPR compliance at PeopleDoc
Get the details on how PeopleDoc became GDPR-compliant and learn from our experience.

READ NOW

eBook

A Practical Guide to Proactive HR Compliance
Learn how to easily manage compliance with the help of technology.

READ NOW

Answers: 1. 4% - 2. Legal basis - 3. Minimization - 4. 72 - 5. Data portability - 6. Access - 7. Delete - 8. Everyone

PeopleDoc by Ultimate Software

PeopleDoc by Ultimate Software is committed to putting people first. The PeopleDoc HR Service Delivery platform helps HR teams upgrade the employee experience, improve HR agility, and ease compliance management. PeopleDoc global cloud solutions provide employee case management, knowledgebase, process automation, employee file management, and eVault capabilities.

Delivered 100% software as a service, PeopleDoc solutions integrate with a wide range of HR and enterprise systems and can be implemented in 8–12 weeks. PeopleDoc is part of Ultimate Software, a leading global provider of cloud-based human capital management solutions. Known for its "People First" culture, Ultimate has ranked in the top 25 on Fortune's U.S.-based *100 Best Companies to Work For* list since 2012, and #1 on Fortune's *Best Workplaces in Technology* list, in the "Large Companies" category, since 2016. Ultimate employs more than 5,600 professionals and serves approximately 6,600 customers worldwide.

More information about PeopleDoc by Ultimate Software can be found at www.people-doc.com.

Learn more

people doc BY ULTIMATE SOFTWARE

www.people-doc.com • contact@people-doc.com