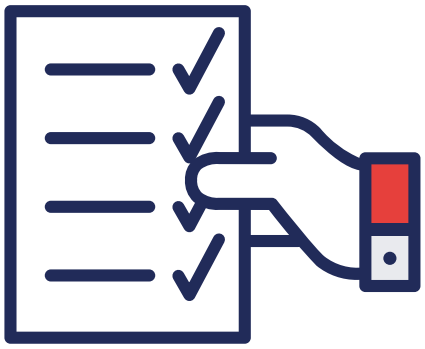
Sympa



The HR GDPR Checklist

This document is meant to help you track down the systems in which you are storing data and to determine whether your organisation's policies for storing that data are aligned with the EU regulations around data security.
This checklist also contains helpful questions to determine whether your partners are complying with the regulation.

Privacy Rights

Question	Why should this question be asked?	Yes	No	No idea
Is it easy for **people** to request and receive all the information you have about them?	People have the right to see what personal data you have about them and how you're using it.			
Is it easy for people to correct or update inaccurate or incomplete information?	People have the right to obtain a rectification of inaccurate personal data concerning them.			
Is it easy for people to request to have their personal data deleted?	People generally have the right to ask you to delete all the personal data you have about them. You should be able to honor this request within about a month.			
Is it easy for people to ask you to stop processing their data?	Your data subjects can request to restrict or stop the processing of their data temporarily if certain grounds apply.			
Is it easy for people to receive a copy of their personal data in a format that can be easily transferred to another company?	GDPR requires that you should be able to send peoples' personal data in a commonly readable format either to them or to a third party they designate. This represents the GDPR's idea that people own their data, not companies.			
Is it easy for people to object to you processing their data?	If you're processing their data for the purposes of direct marketing, you have to stop processing it immediately. Otherwise, you may be able to challenge their objection if you can demonstrate compelling legitimate grounds.			
If you make decisions about people based on automated processes, do you have a procedure to protect their rights?	You need to tell people that you're collecting their data and why. You should explain how the data is processed, who has access to it, and how you're keeping it safe. This information should be included in your privacy policy and provided to data subjects at the time you collect their data.			

Data Security

Question	Why should this question be asked?	Yes	No	No idea
Is your data encrypted, pseudonymised, or anonymized wherever possible?	The GDPR requires organisations to use encryption or pseudonymisation whenever feasible.			
Do you have measures in place that enable subsequent checking and verification of the identity of the person who has recorded, altered or transferred personal data?	If you confront a personal data breach targeted at an information system, you have a documentation obligation which includes the information system's log data from the time of the breach.			
Do you have internal measures in place for preventing unauthorised access to personal data?	GDPR requires that personal data is processed in a manner that ensures appropriate confidentiality of the data. That includes preventing unauthorised access to or use of personal data and the equipment used for the processing.			
Do you have measures in place that ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data?	Your systems and software need to be prepared for data breaches. GDPR demands that you have ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident.			
Do you have a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing?	GDPR regulates that those technical and organisational measures shall be reviewed regularly and updated where necessary. If you are using a Processor, it should assist your organisation in ensuring compliance with this obligation.			

Question	Why should this question be asked?	Yes	No	No idea
Do you have a process in place to notify the authorities and your data subjects in the event of a data breach?	If there is a data breach and personal data is exposed, you are required to notify the supervisory authority within 72 hours. You are also required to quickly communicate data breaches to your data subjects unless the breach is unlikely to put them at risk. If you are using a Processor, it should assist your organisation in ensuring compliance with this obligation.			

Accountability and governance

Question	Why should this question be asked?	Yes	No	No idea
Have you signed a data protection agreement between your organisation and third parties that process (HR related) personal data on your behalf?	GDPR requires that processing by a processor is governed by a contract. The Regulation has a detailed list of things that the parties must agree on.			
In case your organisation is outside the EU, have you appointed a representative within one of the EU Member States?	If you process data relating to people in one particular member state, you may need to appoint a representative in that country who can communicate on your behalf with data protection authorities.			
Have you appointed a Data Protection Officer?	There are three circumstances in which organisations are required to have a Data Protection Officer (DPO), but it's not a bad idea to have one even if the rule doesn't apply to you. The DPO should be a real expert on data protection.			

Lawful basis and transparency

Question	Why should this question be asked?	Yes	No	No idea
Have you conducted an information audit to determine what information you process and who has access to it?	Organisations that have at least 250 employees or conduct higher-risk data processing are required to keep an up-to-date and **detailed list of their processing activities** and be prepared to show that list to regulators upon request. Organisations with fewer than 250 employees should also conduct an assessment because it will make complying with the GDPR's other requirements easier.			
Have you carried out a Data protection impact assessment (DPIA)?	GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons. *If you are using a Processor, it should assist your organisation in ensuring compliance with this obligation.*			
Have you provided clear information about your data processing and legal justification in your privacy policy?	You need to tell people that you're collecting their data and why. You should explain how the data is processed, who has access to it, and how you're keeping it safe. This information should be included in your privacy policy and provided to data subjects at the time you collect their data.			

Sympa's HR Software is created to comply with the GDPR's principle of "**Data protection by design and by default**".

sympa.com