GDPR Guide For Recruiters

employertube

e-Book 2019

Table of Contents

04

GDPR Aim & Its Basic Terms

05

What is Personal Data?

06

Key Elements that will Affect Recruitment

07-10

How does GDPR directly impacts recruitment process

12-15

How Employertube helps recruiters ensure GDPR Compliance

employertube

Aim of GDPR

The aim of the GDPR is to establish a modern and harmonised data protection framework across the EU. The new framework imposes strict duties on employers in relation to the processing of personal data, with potentially very large fines for a breach of the rules (up to €20 million, or 4% of the organisation's total worldwide annual turnover if higher).

GDPR applies to data controllers and processors, as an employer receiving applications you fall into both categories.

What are the basic GDPR terms and how do they relate to recruiting?

In respect to the recruiting function, the GDPR refers to:

Candidates or "data subjects." Candidates are the data subjects because they can be identified through personal data they give to companies. For example, their resumes may include their names, physical addresses or phone numbers. GDPR exists to protect this kind of data. Members of hiring teams are also considered data subjects under GDPR, but their own data will not be processed in the same extent that candidate data will.

Employers or "data controllers." Employers, or recruiters who serve as their company's main representatives to candidates, determine the purpose of collecting candidate personal data. This makes them the data controllers who are fully responsible for protecting candidate data and using it lawfully.

Applicant Tracking Systems (ATS) and other recruitment software/services or "data processors." Your ATS is a data processor because it processes candidate data on behalf of your company following your company's instructions. Data processors often have "sub-processors" (e.g. Workable uses a cloud platform to deploy its system.)

So What is Personal Data?

The European Commission has said:

“Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.”

So it’s not just about handling personal data such as names, addresses and CVs its goes that step further to cover any data held that covers race, ethnicity, religion or even a simple photograph. If you handle and store data about people, you are responsible for its safe keeping and security as well as ensuring the right people have access to it. You also need to apply the necessary control over how you share this information with others, as again you will be held responsible for how third parties use and protect the data.

It's all about consent

One of the fundamental changes is around explicit consent. It will need to be explicitly clear when data is being collected and how it will be used. You can't have a tick box that covers everything with lots of terms and conditions in small print. You will need to be able to prove that the person whose data you hold has agreed to have their data collected, stored and used.

Access requests

GDPR puts the power back in the hands of the individual therefore if you receive an access request, where an individual requests to know what data you hold about them, you have to provide the information within one month and you cannot request payment for doing so. Allowing candidates access to review and update their data at any time, with the option to ask for updates, will also be key.

The right to be forgotten

Companies will need to make sure that everyone is given the ability to withdraw their consent to being contacted at any time and are given the right to be forgotten. This means that individuals can ask for their personal data to be deleted from your system at any time.

The paper trail

One of the most significant criteria of GDPR will be the need for a 'paper trail' regarding your data management. It is paramount that you have a centralised system that handles all candidate data and allows the monitoring of how data is being collected, stored and used

How does GDPR directly impact the recruitment process?

- Under the Regulation, when an employer collects personal data about an applicant during a recruitment process, whether this is directly from the applicant or from a third party such as a recruitment agency, it must provide the applicant with an information notice, also known as a privacy notice or fair processing notice.

- This notice must set out certain required information, including the purposes for which the data will be processed, the legal bases for processing and the period for which the data will be retained. The employer could provide the information notice on its website, send a link or copy of the notice in correspondence to individual applicants. Where the employer uses a third-party recruitment portal, it could ensure that the details of the vacancy include a link to the information notice

- Candidates have the right to request viewing, deletion of; information on and access to personal data held on them, it is mandatory to provide this information and should be supplied within one month of request. This new protocol has been set in place to protect clients/candidates and grant them more control over who stores their personal information, and how it is used. A detailed privacy notice must be accessible to candidates explaining how their data will be handled.

Candidate Consent

The way consent works will be changing. Implied consent will no longer be enough for recruiters obtaining information through online profiles, candidates will need to give explicit consent for their information to be put forward for a position they did not directly apply for. Any data collected, stored, shared or used needs to be relevant to the position applied for and legally justifiable. Personal information collected with consent cannot be used for a different purpose than that of the given consent, SMS and the candidates must also opt email marketing in separately.

Data

The way personal data is stored within a company needs to be updated, this means creating a centralized system where all candidate data is stored. Having all your contacts in one location will facilitate paper-trail creation, which will be a legal requirement. From obtainment, to storage, to use; all data movement in and out of the company needs to be documented, this includes

Retention of data

Employers should put in place policies setting out for how long recruitment data will be retained. The employer will need to retain some candidate data for the purpose of responding to potential employment tribunal claims arising out of the recruitment process. The employer should retain only the minimum data required for this purpose and only until the relevant limitation periods have expired. If the employer intends to keep the details of unsuccessful candidates on file for future recruitment rounds, it must notify them of this in the information notice. It should either obtain the candidates' consent, or notify them of their right to object (if it relies on its legitimate interests as the legal basis for processing).

The policy should cover how the employer will deal with unsolicited personal data, for example CVs submitted on a speculative basis. The policy could state that if the employer receives an unsolicited CV at a time when it is not recruiting, it will delete the CV and inform the candidate of this. If the employer holds unsolicited CVs on file for future recruitment rounds, it must inform the candidates of this in a privacy notice, along with the other required information.

Candidates have the right under the GDPR not to be subject to a decision based solely on automated processing, for example automated shortlisting where candidates without a particular level of qualification are automatically filtered out before the applications are considered by the recruiters. Under the GDPR, employers can use automated decision-making only if it is:

With GDPR

Candidates have more rights than previously covered by the Data Protection Act. However, if your company has aligned your processes and systems with the Data Protection Act, you're already in a strong position to comply with GDPR. Essentially it all comes down to knowing exactly what personal data you process, where it is, and why you need it. Candidates have the following key rights:

The right of access:

The right to access their personal data; have confirmation that your company is processing it; and also access any further data that pertains to theirs, is already set out in the Data Protection Act. However, with GDPR there are a couple of differences. The first is that you cannot charge for this information, previously candidates might pay a £10 access fee. The second is that you must respond much faster to their request than before - within a month. This highlights the importance of having a clear picture of where all the data your company processes is stored, so you can access it quickly.

The right to be informed:

Under GDPR you must 'provide fair processing information'. Informing candidates that you are processing their data, and how you do it. Most companies will already have a Privacy Notice that sets this out, providing candidates with a link to this from an online application form is the best way to ensure they are informed. Of course, you may have sourced a candidate in a different way; perhaps at a networking event, on LinkedIn or via a recruitment agency. In this case you must provide fair processing information within one month, for example by emailing them and providing a link to your company Privacy Notice. Check that your Privacy Notice includes all the information required by GDPR.

The right to rectification:

Having requested information if a candidate spots an error they have a right to have this error rectified within one month. For example if your data contains an incorrect job title, current salary, or wrong contact details, you will need to amend this quickly. Companies that have large recruitment volumes may find that it is easier to allow candidates to access and rectify their data themselves. Providing candidates with a log in to their personal profile (a candidate portal) is a good way of managing this, and they can also update CVs and other information at their own convenience.

The right to be forgotten (or erasure):

. Your candidate database is an important asset but a key requirement of GDPR is that candidates can have their personal data removed if they wish. Again, the time limit for this is one month, although there are some reasons where you can refuse. For example, you may need to retain personal data to comply with a legal obligation, or if you're processing their data 'for the performance of a task carried out in the public interest or in the exercise of official authority.' While it most likely that candidate data will not be exempt from a request for erasure, you can find more information about this here.

GDPR And Consent

- A key aspect of GDPR that you have probably come across is ‘consent’. You may have interpreted this as that candidates need to give you consent to process their data. This is true for certain types of activities. For example if you planned to add a candidate to your marketing list in the hope that they might buy your products or services, as well as apply for a job!
- However in terms of recruitment, consent to process their data is given implicitly when they apply for a role or upload their details to your candidate portal. Naturally, you must only process this data for this purpose. In GDPR this comes under being ‘able to demonstrate a legitimate interest’, i.e. that you need to process their data in order to shortlist them for interview, or identify the right opportunity for them.

- Best practice for recruitment agencies is to get consent from candidates to process their data, and especially to pass it on to third parties, i.e. our clients / potential employers. It is worth checking with any recruitment agencies that you work with, that they have got consent from candidates before handling this data. This will provide your business with additional protection against non-compliance.

- Of course, another really important aspect of GDPR is that you have the right systems and process in place to protect your candidates’ personal data. Often this data contains quite sensitive information that could be used in identify theft, or for malicious reasons. A high profile candidate, whose job search is private, will not want this information getting out into the public domain. As well as risking possible fines for non-compliance in the event of a breach, your company can also suffer considerable reputational damage; as well as the damage it might do to relationships with candidates and employees. Make sure your data is secure.

How Employertube helps recruiters ensure GDPR Compliance

GDPR Compliant Video Interview Platform

Employertube is video interview platform that serves to ensure that recruitment organizations are fully GDPR compliant. We provide a transparent platform where recruiters have access to tools and processes that will ensure compliance.
Unlike old fashioned methods our platform helps manage data in one place making it easier to securely manage data.
The platform records candidate consent, helps keep data accurate, records requests to delete data and allows you to keep records securely. It also ensures that data is only used for the purpose it was collected for by recording and limiting access.
Data is deleted from the platform once its confirmed that its no longer required for the job application process.

Option to add your company privacy, terms and conditions

Employertube video interview software is provided in the look and feel of our customers. We provide the option for clients to add their own privacy policy, terms and conditions.

Employertube Video Interview Software Supplier

We adhere to The Sytorus DPEA 7 Data Management Principles of GDPR.

Fair, Transparent & Lawful Processing

Ensuring that we acquire personal data in a fair and transparent way and have a legal basis to do this

Purpose Limitation

We only use the personal data for the purpose that it was specified to the data subject

Minimization of Processing

We only collect the personal data from data subjects that is required.

Data Accuracy & Quality

We proactively ensure that personal data is accurate and up-to-date and supply the tools for our clients to maintain accurate records

Retention/Storage Limitation

Our systems ensure that we do not keep personal data for too long

Security & Confidentiality

We have a robust online and physical security managed by Amazon Web Services (AWS) AWS offer state of the art security and has certification for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2014, and ISO/IEC 9001:2015. Read more :

Accountability & Liability

AWS offers a GDPR-compliant Data Processing Addendum (GDPR DPA), enabling Employertube to comply with GDPR contractual obligations. The AWS GDPR DPA is incorporated into the AWS Service Terms, and the DPA applies automatically to all customers globally who require it to comply with the GDPR.

Data controllers and staff are trained in data management principles. Employertube is operated by Adfuture Ltd who are registered with the Information Commissioners Office (ICO) . The ICO is the UK's independent body set up to uphold information rights. Our certificate registration no. ZA307541

Video Interview Platform Practical Solutions

- Candidate Permissions
- Our system ensures we seek consent to record interviews
  a. Before process begins
  b. Before candidate selects record.
-
- Candidate access to data
- Candidates are provided with a dashboard where they can see the data that is being held.
- Candidates are given the tools to request deletion of their data from our system

Use of Candidate data

Candidate data is essentially our clients data and Employertube will only use this to
To enable to service the candidates account.
Employertube proactively request the deletion candidate data from its clients and its up to the organization to justify keeping the data.

Candidate Consent (GDPR compliant consent)

How a recruiter gains consent when performing a video interview is extremely important. For consent to be GDPR compliant, Employertube offer a clear explanation of the intended processing of their personal data (the Fair Processing Notice).
If the intention to film and record the individual is raised once the recording has started, the permission is likely to be deemed inadequate and non-compliant. The approval must be requested before filming when there is no pressure for the candidate to agree, and where the candidate still has the option to decline.
To adhere to GDPR compliance Employertube makes it impossible to commence the recording until the candidate has read and agreed to the terms and conditions.
Once approved, the webcam connects, but the recording won't begin until the candidate has been briefed and appropriately informed.
Storage (GDPR compliant storage of a video interview)
There are a specific set of storage requirements that a video interview software company must follow. The recording can’t be randomly thrown in an online folder, it must be placed in a designated, safe and access-controlled environment.
Employertube data structure and AWS

Data Deletion

When choosing a video interview software, it's important to check the company have the appropriate functions that allow you to delete your recordings when necessary. Employertube provide these tools both to recruiters and candidates

Under the storage limitation principle of GDPR (Principle 5), the organization must not retain any data if you no longer require it for the purposes defined and agreed upon.

Our video interview platform provides the tools required to delete recordings, and we are proactive about keeping data up to date.


Follow us on:
employertube