GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

*Webinar on*

# The General Data Protection Regulations (GDPR) and its impact on Recruiting

# Learning Objectives

- *What the General Data Protection Regulations require from employers*
- *What are data controllers and data processors and what employers must do with them*
- *Changes for Applicant Tracking Systems, Recruiting software and other data tools*
- *Data mapping under GDPR*
- *Policies and procedure changes*
- *Legal implications and how to protect yourself*

To be able to apply recruitment GDPR properly, you need to understand such concepts as “personal data,” “data controller,” and “data processor.”

**PRESENTED BY:**

*Dr. Chartier is the Principal of HRinfo4u, a human resource consulting firm, and a well-known educator and speaker. As a consultant, he works with organizations to improve the effectiveness and efficiency of their human resource function. He has worked extensively in designing, developing and implementing human resource programs, procedures, and systems for smaller and mid-size firms up and down the Hudson Valley.*

GRC Online Training Hub EDUCATORS
Axons Technology and Solutions

On-Demand Webinar

Duration : 90 Minutes

Price: $200

# Webinar Description

Data protection in recruitment has always been taken seriously, as the breach of employee data protection policy is an integral part of any corporate protocol. However, the introduction of GDPR changed the subject completely by offering an entirely different perspective on the data flows in companies. Thus, making recruitment GDPR-compliant requires much more than a simple change of some policy. GDPR makes a great impact on it, it requires a broader cultural change in companies based on awareness of data sensitivity and the importance of keeping it intact.

Recruitment and GDPR are very closely tied since HR managers handle large volumes of candidate data during the hiring and firing processes. Therefore, they face the need to manage increasingly large volumes of personal data that often remain dramatically unprotected. What could be previously tolerated to a certain degree is now illegal; hence, not to breach the laws of data protection in recruitment and to avoid litigation on these grounds, companies now struggle to adapt to the GDPR-induced changes.

Data protection in recruitment has always been taken seriously, as the breach of employee data protection policy is an integral part of any corporate protocol. However, the introduction of GDPR changed the subject completely by offering an entirely different perspective on the data flows in companies. Thus, making recruitment GDPR-compliant requires much more than a simple change of some policy. GDPR makes a great impact on it, it requires a broader cultural change in companies based on awareness of data sensitivity and the importance of keeping it intact.

Recruitment and GDPR are very closely tied since HR managers handle large volumes of candidate data during the hiring and firing processes. Therefore, they face the need to manage increasingly large volumes of personal data thTo be able to apply recruitment GDPR properly, you need to understand such concepts as “personal data,” “data controller,” and “data processor.”

When we speak of personal data covered by the GDPR, this includes any personally identifying information like a personal name, a photo, an email address, or even the person's posts in social networks. Other examples of personal data covered by recruitment GDPR include his/her banking details, details of the medical record, and even the computer IP address. Thus, under GDPR, all data subjects (that is, EU citizens) have data rights such as breach notification, right to access, right to be forgotten, data portability, and privacy by design.

Data controllers under the GDPR are entities authorized to determine the purposes, conditions, and means of personal data processing. In other words, a controller is a person or business organization able to use personal data for specific purposes in compliance with GDPR.

Data processors are entities that hold personal data on behalf of the controllers. Thus, a processor is a recruiting firm holding a database of candidate resumes or the company employing staff and storing their personal records. At often remain dramatically unprotected. What could be previously tolerated to a certain degree is now illegal; hence, not to breach the laws of data protection in recruitment and to avoid litigation on these grounds, companies now struggle to adapt to the GDPR-induced changes.

Recruitment GDPR rules have affected recruitment and recruitment agencies to a large degree. It is hard to deny the fact that GDPR has actually made the work of recruiters harder by creating additional challenges and risks in the process. Here are the most important issues to keep in mind when thinking of GDPR and recruitment:

## Requirement Apps and Tools

It's imperative to update the recruitment software currently used, with new privacy requirements in mind. This change is costly and time-consuming, while recruiters will also need some training and time to learn to navigate new programs. Thus, the process of recruitment may stall for the transition period.

## New Rules for Data Mapping

Recruiting firms have to conduct thorough data mapping now by determining which candidate data is collected in the recruitment process, through which processing stages it goes, and where it is stored. If you have a separate recruiting department, the process of establishing data mapping as a new procedure may take quite a lot of time and effort.

## New Legal Policies

It’s necessary to update your corporate page with vacancy announcements by adding a GDPR-compliant privacy policy and determining the ways in which a candidate may turn to you regarding his/her personal data protection.

## Recruitment Agency Evaluation

If you don’t have a recruitment department and rely on the assistance of external recruitment firms, be sure to check their policies regarding GDPR compliance. It’s imperative to work only with firms that comply with GDPR to avoid employment litigation.

## More Complex Recruitment Workflow

According to GDPR, all personal data should be removed from the company’s database after the job interview (upon the candidate’s request). So, for larger companies, this means harder recruitment because of slower processes and inability to store candidate data for easier recruitment for new opening vacancies.

## Selective Data Collection Requirements

GDPR allows the collection of personal data only for active vacancies and only about people with whom a job interview will be held.

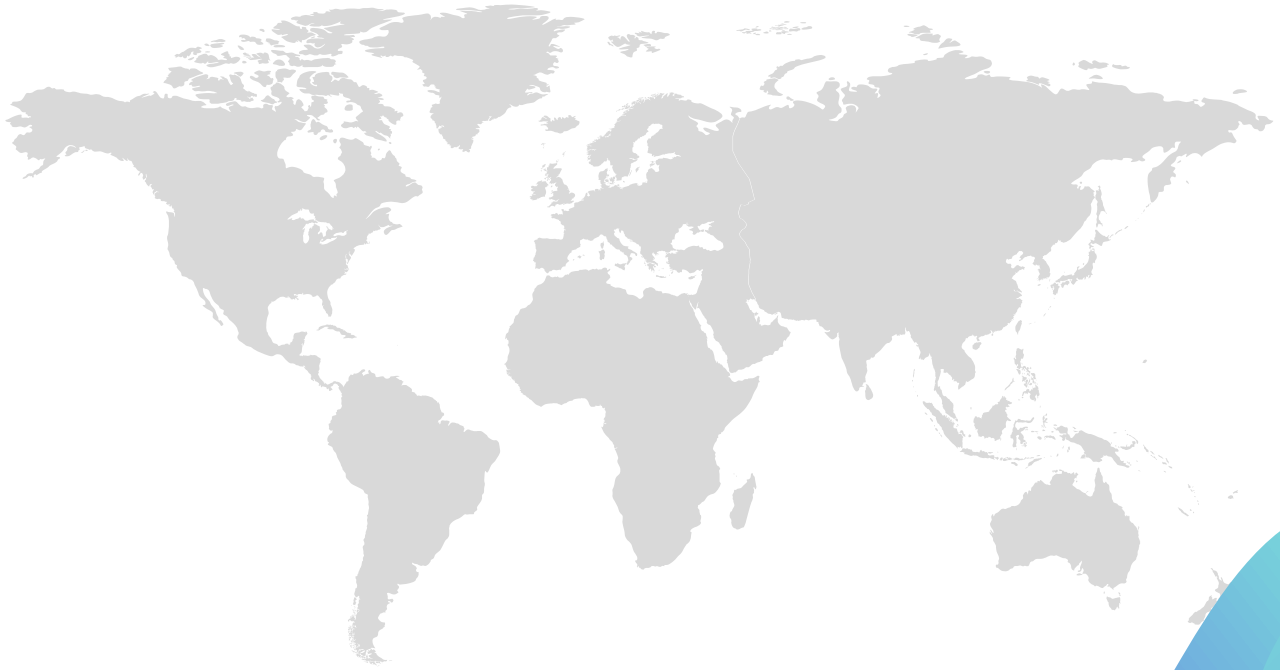
It is important to keep in mind that even though individuals may post their personal data in social profiles like LinkedIn, recruiters do not have the right to retrieve and store that data in their databases; they need to ask candidates for permission to process their personal information by indicating a specific purpose of data use and clarifying the procedure by which the candidate may withdraw that consent. Such changes will definitely complicate recruiters' work, as the latter used to store some "hot candidates" list for specific positions and contact the most suitable candidates in case a proper vacancy arises.

The General Data Protection Regulation (GDPR) was adopted by the European Union (EU) in April 2016 and replaced the EU Data Protection Directive 95/46/EC. The GDPR introduces new obligations to data processors and data controllers, including those based outside the EU. Given that infringement can lead to fines of up to 4% of annual worldwide turnover or €20 million, it is important for companies to assess how the GDPR affects them and be compliant from May 2018 onwards.

There are many aspects to be considered to ensure full compliance. For example, there are requirements for explicit consent to be freely given by individuals for their data to be used for specific purposes, as well as the right for individuals to request details of information held and for data to be deleted. Some organizations need to carry out assessments, ensure effective procedures are in place and designate a Data Protection Officer to meet new accountability requirements.

# Who Should Attend ?

*Recruiting managers*
*Recruiters*
*Talent acquisition specialists*
*Human Resource Managers and Supervisors*



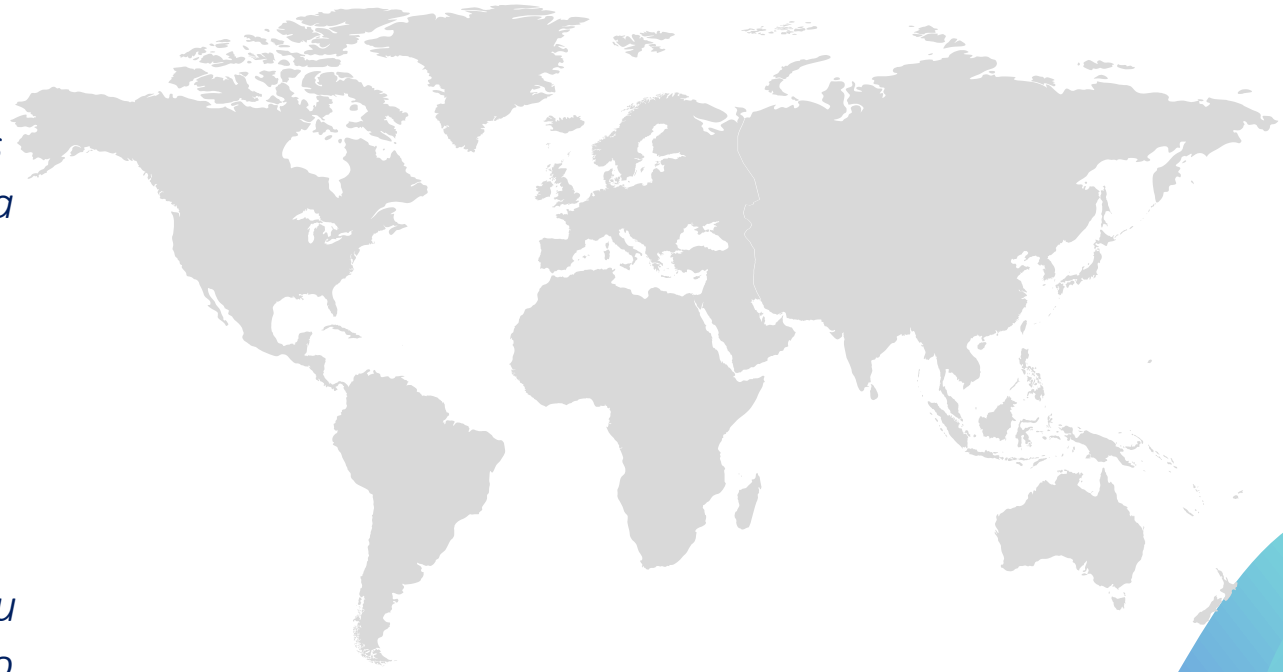
GRC EDUCATORS
Online Training Hub
Axons Technology and Solutions

# Why Should Attend ?

*Pretty much every business must comply with the EU's data laws, even if they're based in the US. This is because most companies have at least some data belonging to EU citizens stored on their servers. In order to process that data, the organization must comply with GDPR principles.*

*However, if you truly have no dealings with the EU, you can avoid having to comply with using a traffic filter. By blocking any EU traffic to your website, you can make sure that only non-EU traffic is allowed to your website and only those outside Europe can enter their details onto your site.*

*One of the requirements is to have a data controller and a data processor for every organization. There's a distinct difference between a data controller and a data processor, as stipulated by the EU.*



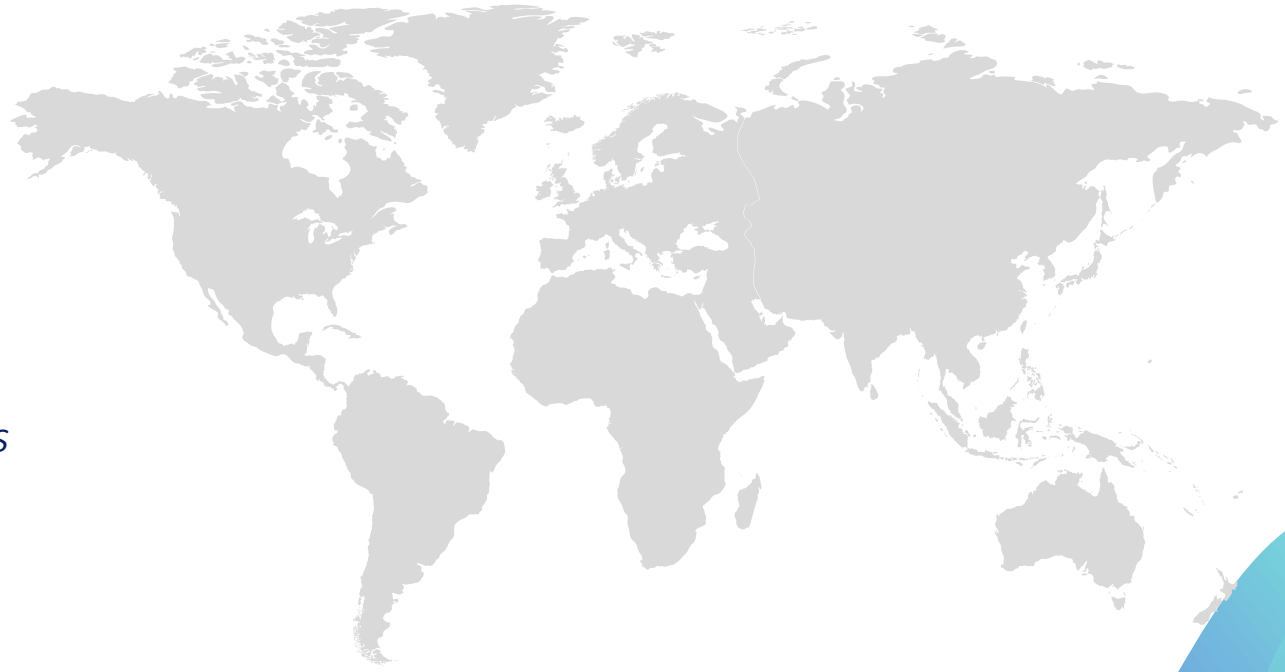
GRC Online Training Hub EDUCATORS
Axons Technology and Solutions

*A data controller is responsible for setting out how and why data is collected but doesn't necessarily collect the data itself.*

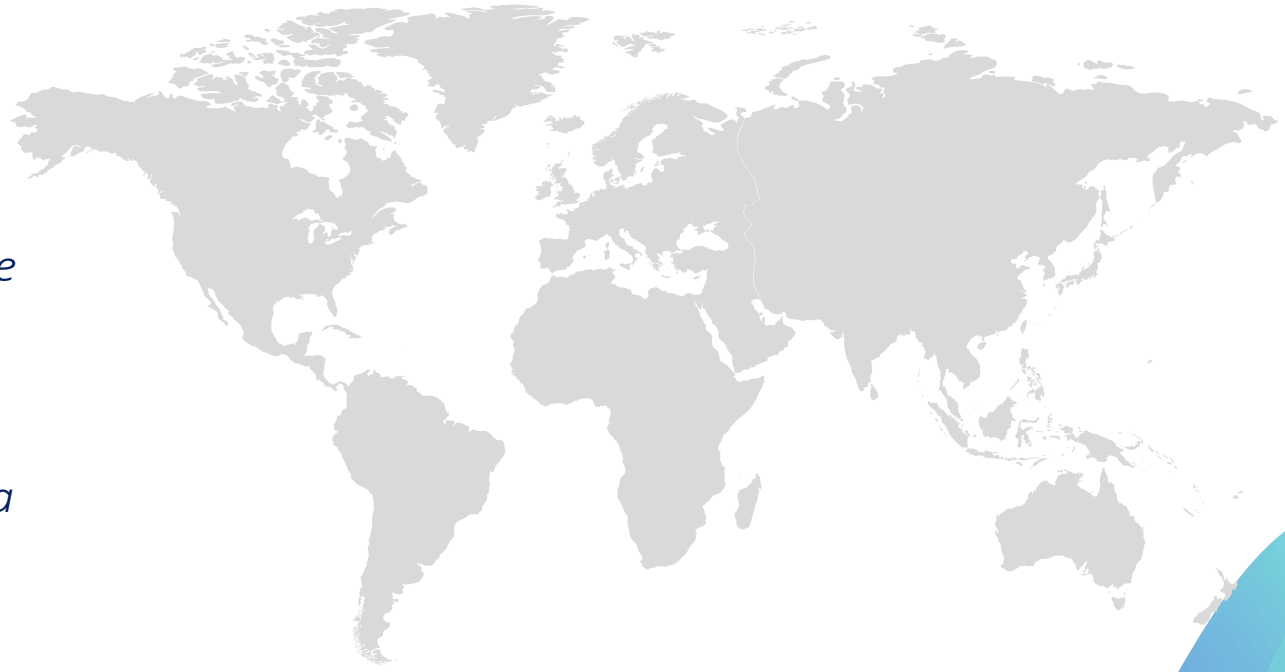
*That means a controller could be any organization, from a small retailer to a global manufacturing giant to a not-for-profit, while a processor could be an IT services firm they employ.*

*It's the controller's job to make sure the processor complies with data protection law, while processors must maintain records of their processing activities to prove they abide by rules. Unlike older data protection laws, both the controller and the processor are jointly liable for financial penalties in the event of a data breach or if the processor is found to have handled data illegally.*

*It is possible for a non-EU-based controller to use an EU-based processor, in which case all parties need to be compliant with GDPR.*



GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions



*GDPR states that controllers must make sure it's the case that personal data is processed lawfully, transparently, and for a specific purpose.*

*That means people must understand why their data is being processed, and how it is being processed, while that processing must abide by GDPR rules.*

*Consent must be an active, affirmative action by the data subject, rather than the passive acceptance under some models that allow for pre-ticked boxes or opt-outs.*

GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

To register please visit:

**www.grceducators.com**
**support@grceducators.com**
**740 870 0321**