A guide to employee onboarding and GDPR compliance

Five ways to ensure effective handling of new hire data

webonboarding

always exceed expectations

The smart approach to GDPR compliance

Data privacy is a complex area of legislation. A simple overview of the European Union's recent GDPR (General Data Protection Regulation) law runs to hundreds of pages, across eleven chapters.

While these laws apply only to EU countries, the global nature of business means that they have effectively raised the bar for the way data privacy is legislated throughout the world.

This poses a considerable challenge for HR managers tasked with making sure that the way employee data is being collected, managed and stored is fully compliant with GDPR level of standards.

This responsibility starts the moment a successful applicant is chosen, it's why employee onboarding plays such a vital role in shielding companies from data protection risks.

An effective compliance strategy requires a solid understanding of the key principles contained within GDPR and having the tools needed to effectively manage and monitor employee information.

This guide provides practical business information and advice on how to work towards privacy data compliance within your company. This guide looks at five key GDPR principles which impact on employee onboarding. It includes:

1. Lawful and Transparent
2. Data Minimisation
3. Accurate Data
4. Storage Limitation
5. Confident and Secure

Plus:

- An overview of each of the main principles
- The onboarding challenges they pose
- The actions required to work towards compliance

We will then examine the role that technology and cloud-based systems are playing in helping HR teams to meet the GDPR requirements. With maximum fines of €20 million, it's an area of operations that you can't afford to get wrong.

1. Lawful and Transparent

Be clear about what data is collected and why.

What's the principle?

The General Data Protection Regulation (GDPR) places a responsibility on companies to be clear about why data is being collected from employees and exactly what that data will be used for.

You must identify the 'lawful basis' that justifies the collection and use of personal data and be clear, open and honest with new hires from the start about how you will use their data.

As part of this commitment, employees have the right to see exactly what information is being held on them in the form of Data Subject Access Requests (DSAR).

How does it impact onboarding?

From the moment onboarding starts, incoming employees must be made fully aware of an organisation's GDPR policy. Company privacy policies must be shared and explained to new hires before any personal data is collected.

HR teams must also have adequate processes in place to quickly deal with DSAR requests. This becomes difficult when employee information is held in multiple formats - emails, spreadsheets and paperwork.

This makes collating information slow and inefficient with problems of data management increasing as companies grow and the volume of information being held increases.

Actions required

- Make sure GDPR policy is provided from the start of onboarding process
- Provide clear information on what data is being collected and why
- Establish a robust HR process that can handle DSAR requests

FACT: More than two-thirds (68%) of HR teams still use manual methods (email/post) to manage new hire information. *

* data: webonboarding, 2018

2. Data Minimisation

Collect only employee data that's necessary for the role.

What's the principle?

This requires you to collect only 'essential' personal information and to avoid anything that could be considered extraneous.

For each dataset collected, an organisation needs to designate a specific purpose - why do you need it?

All personal data needs to be:

- Adequate - sufficient to achieve the purpose
- Relevant - has a rational link to the purpose
- Limited to what is necessary - only what's needed for purpose

The GDPR regulations require organisations to be able to demonstrate that they have effective processes in place to monitor and maintain the data minimisation principle.

How does it impact onboarding?

Any kind of 'one-size-fits-all' approach to paperwork will create potential compliance risks. Often general new hire documentation can be liable to collect data that's not necessary for each specific role.

HR teams also need to understand that data minimisation is an ongoing task with the data that's 'necessary' evolving over time as employees' responsibilities and status changes.

Without a robust data management process, the removal of irrelevant or unrelated information becomes a headache with outdated details and legacy documents being left in the system.

Actions Required

- Specify a necessary purpose for each dataset
- Avoid risks of 'one-size-fits-all' paperwork approach
- Ensure you have robust data management processes

3. Accurate Data

Ensure employee information is accurate and valid.

What's the principle?

This places a responsibility on HR managers to ensure that any onboarding information collected is accurate, valid and fit for purpose.

Adequate processes must be in place to ensure data accuracy and to identify incorrect, outdated or misleading data. Employees have the right to challenge the accuracy of information and mistakes need to be quickly rectified.

It is advised that a record is kept to show any challenges that are made about the accuracy of employee data and to document the actions this resulted in.

How does it impact onboarding?

To work towards compliance, the principle relies on efficient and reliable data management processes. This is difficult to achieve when onboarding is often handled manually and data collected in multiple formats - emails, texts, paperwork.

The need to transfer information by hand means that errors and mistakes become unavoidable. The more new hires being handled, the greater this compliance risk becomes.

The fragmentation of data hampers the ability to deal quickly with any challenges and heightens the risk posed by inaccurate duplicate and legacy information being left in the system.

Actions required

- Update and automate processes - minimise risks of human error
- Create clean, accurate and accessible datasets
- Introduce processes for data to be challenged and checked

4. Storage Limitation

Data must be relevant and removed when no longer necessary.

What's the principle?

This requires you not to keep personal data any longer than is necessary. If the original purpose for the information being collected is no longer valid, all of that data needs to be removed.

This could be as a result of changes to a role or simply as a result of employees leaving the organisation. How long you keep each form of data needs to be clearly documented and made accessible to employees.

How does it impact onboarding?

With an increasingly flexible workforce and more varied forms of employment, ensuring that outdated information is removed is a major challenge.

Particularly risks are caused when onboarding is managed manually with information spread across an organisation in the form of documents, spreadsheets, emails and texts.

This fragmentation of data makes it hard for HR teams to keep tabs on which information remains active and necessary. It also creates the risk of duplicate datasets existing - causing outdated data to remain in the system.

Actions required

- Identify length of time each dataset is needed
- Robust data management - prevent information scatter
- Automate data processes - synchronise and streamline handling

5. Confidential and Secure

Accept full responsibility for data security.

What's the principle?

This emphasises the responsibility to ensure the 'confidentiality, integrity and availability' of any personal data that's collected or stored by HR.

This requires assessing the security risks that are posed by each of the HR processes that you have in place. If things go wrong, what are the consequences and how can you adapt your operations to mitigate the risks?

Measures must be taken to allow personal data to be quickly restored in the event of any physical or technical incident. Processes should also be in place to test the effectiveness of your security.

How does it impact onboarding?

Any kind of data management failings pose a risk in terms of data security. Tight control needs to be maintained on who has access to personal data.

Manual handling of information poses specific problems with documents having to be posted between HR, hiring managers and new hires. This creates the common problem of paperwork being lost in the post.

The way data is stored must also be considered with physically held information being at risk from property theft, as well as fire and water damage.

Actions Required

- Analyse security risks of your onboarding processes
- Minimise reliance on physical data storage/exchange
- Ensure robust system of document access and control

Tools to help your employee onboarding processes become more GDPR compliant

Automated processes and cloud-based management.

Analysis of the key GDPR principles highlights a basic need for robust, efficient and fast ways to manage employee onboarding information. It's something which traditional onboarding approaches struggle to meet.

Onboarding starts from the moment a role has been offered and covers all of the HR related tasks that are required, right through to a new hire's first days in the workplace.

This is typically managed via paper-based processes and the manual handling of bulk data. It creates a compliance weakness as data becomes fragmented across a mix of emails, documents, texts and spreadsheets.

Webonboarding has been developed to provide HR and hiring teams with a much more efficient and streamlined way to access, monitor and manage any personal information relating to onboarding new hires.

It removes the need for manual onboarding tasks with all of the information exchanged between HR, hiring managers and incoming employees being handled digitally, allowing for fast and efficient automated processes.

It reduces the risk of errors and mistakes being made and removes the need for documents to be physically moved between different locations - eliminating the danger of data sensitive documents being lost in transit.

How webonboarding helps you become more GDPR compliant.

Here's a look at how webonboarding provides the tools needed for effective compliance with each of the key GDPR principles:

1 Lawful and Transparent

Real-time data and cloud-based management allows for open and accessible storage for privacy policies.

Webonboarding:
- Integrate GDPR policy documents, such as privacy policies into the onboarding process
- Clear, transparent and audited document control
- Instant access to data - easily handle DSAR requests

2 Data Minimisation

Custom templates and workflows ensure that only 'necessary' information is collected.

Webonboarding:
- Avoid risks of 'one-size-fits-all' paperwork
- Custom templates - role specific documentation
- Accurate onboarding data collection

3 Accurate Data

Efficient, automated digital process reduces human errors and inaccuracies

Webonboarding:
- Automated processes - minimise risks of human error
- Fully scalable - efficient handling of bulk data
- Create clean, accurate and accessible datasets

4 Storage Limitation

Central control of data minimises risks of duplicate and legacy information.

Webonboarding:
- Central data management - prevent info 'scatter'
- Synchronised data - guards against duplication
- Digital timestamp and audit of info

5 Confidential and Secure

Compliance friendly data management controls and paperless processes.

Webonboarding:

- Fully paperless process - remove risks of posting and emailing documents
- Secure cloud-based storage - no fire/theft/damage risks
- Document ownership and audit trail

webonboarding
always exceed expectations

Helping your employee onboarding processes be GDPR compliant.

Find out more about webonboarding at
www.webonboarding.com

Email:
contact.us@webonboarding.com

Tel:
+44 (0) 0800 170 0800

twitter.com/webonboarding

linkedin.com/company/webonboarding