

Whitepaper

Data Sovereignty and HR

In this guide, you'll discover everything you need to create and implement an effective background screening policy for candidates and employees. It covers practical tips, the latest trends, and includes a handy checklist to keep you on track. With these insights, you'll be fully prepared for 2026!

Screening Guide
Table of Contents

Introduction 03

Why Candidate Privacy Demands Rethinking HR Data Practices 04

The Compliance Imperative: GDPR and Beyond 05

Data Sovereignty Challenges for HR Teams 06

Candidate Privacy Concerns in Hiring 07

Strategic Implications for Hiring Teams 08

Screening policy checklist 09

Meet PESCHECK 11

Definition list 12

Introduction

In 2026, data has become both an asset and a risk for HR teams across Europe. The rise of digital recruitment tools, cloud storage, and AI-driven hiring practices has transformed how candidate information is collected, processed and stored. At the same time, regulations like the General Data Protection Regulation (GDPR) and growing emphasis on data sovereignty demand that HR teams take a fresh look at where data resides, who controls it, and how it can be accessed under different legal regimes. Ignoring these realities is no longer just a compliance issue, it undermines candidate trust, employer brand, and legal security.

> "Respecting candidate data is about people. When organizations show they care where and how personal information is kept, they send a clear message: we value you, your privacy, and your trust."
>
> Serhat Elban, CEO PESCHECK

Understanding Data Sovereignty in the EU Context

Data sovereignty refers to the concept that digital information is subject to the laws and governance frameworks of the territory where it is created or stored. This goes beyond simple data storage location, it encompasses who has legal control over data and which jurisdiction's laws apply. In the EU, data sovereignty is entwined with privacy protections that give individuals extensive rights over their personal information, including recruitment and HR data.

Where candidate data is stored or processed can change the applicable legal regime. For example, if an EU candidate's personal information is hosted on servers outside the EU, it may fall under foreign laws that conflict with EU privacy frameworks. This disconnect can create sovereignty gaps that expose organizations to legal challenges and reduce transparency for data subjects.

Why Candidate Privacy Demands Rethinking HR Data Practices

Recruitment inherently involves large volumes of personal information, ranging from CVs, contact details, interview notes, background check results, to psychometric test results and assessment data, all of which fall under GDPR's protections.

Even in everyday hiring operations, candidates are increasingly sensitive to how their personal data is handled. Studies show that a significant proportion of job seekers worry about how organizations manage their personal information, and poor data protection practices directly erode trust in potential employers. For instance:

- ✓ Research indicates that 62% of candidates are concerned about how their data is managed, and mishandled privacy can lead to reputational damage and talent pipeline loss.
- ✓ Companies that experience data breaches can lose as much as 25% of their qualified candidate pipeline within six months as applicants avoid organizations perceived as unsafe with personal data.

For HR teams, this means that privacy practices must be proactive, transparent, and candidate-focused. It is no longer enough to comply with GDPR; organizations must communicate clearly how data is collected, stored, and protected, and ensure that candidates feel safe throughout the hiring process. Doing so transforms privacy from a compliance obligation into a competitive advantage in the war for talent.



The Compliance Imperative: GDPR and Beyond

The General Data Protection Regulation (GDPR) remains the foundation for handling candidate and employee data across the EU. In 2026, however, compliance goes beyond meeting legal requirements, it requires continuous accountability, transparency, and the ability to demonstrate proper data practices at any time.

At its core, GDPR requires that personal data is processed lawfully, fairly, and transparently. For HR teams, this means embedding privacy into every stage of the hiring process and moving from reactive compliance to proactive data governance.

In practice, organizations must clearly explain what data is collected, why it is needed, and how long it will be stored, while applying strict data minimization principles. They also need a documented legal basis for processing and must ensure candidates can easily exercise their rights, such as accessing, correcting, or deleting their data.

What is Important?

- ✓ **Clear communication about data use and retention is essential to transparency**
  Candidates need to understand what happens to their data from the moment they apply. Clearly outlining how information is used, stored, and for how long helps reduce uncertainty and builds immediate trust in the process.
- ✓ **Data minimization reduces both compliance risk and candidate concern**
  Collecting only the data that is strictly necessary limits exposure in case of breaches or misuse. It also reassures candidates that the organization respects their privacy and avoids unnecessary intrusion.
- ✓ **Documented legal bases ensure accountability in case of audits**
  Having a clear and recorded justification for processing personal data demonstrates that decisions are intentional and compliant. This not only supports regulatory audits but also strengthens internal governance and consistency.
- ✓ **Enabling candidate rights builds confidence and reinforces fairness**
  Giving candidates easy access to their data and the ability to correct or delete it shows respect for their control over personal information. When these rights are handled efficiently, it reinforces the perception of a fair and trustworthy hiring process.

Data Sovereignty Challenges for HR Teams

Cross-Border Data Flows

Global HR systems often centralize recruitment technology, analytics, and cloud storage across regions. While this can improve efficiency, it also complicates compliance. If candidate data is stored in a non-EU jurisdiction, local laws may grant foreign authorities or service providers access rights that conflict with EU privacy standards. This creates sovereignty risks that extend beyond GDPR alone.

Vendor and Third-Party Risks

Recruitment technology rarely operates in isolation. HRIS platforms, ATS systems, payroll processors, assessment tools, and background check vendors all act as data processors. Although GDPR holds HR teams accountable as data controllers, a breach or non-compliance by a third party can still result in penalties and reputational damage for the hiring organization. Active vendor governance, Data Processing Agreements (DPAs), and security assessments are therefore essential.

Candidate Rights and Expectations

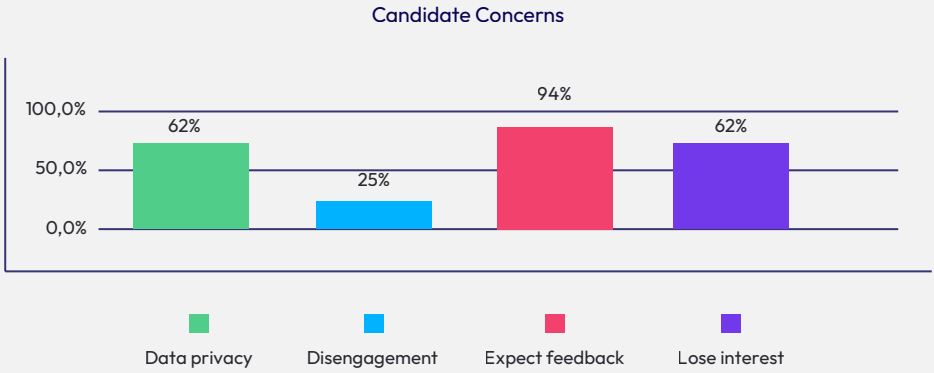
Under GDPR, candidates have extensive rights over their personal data, including access, correction, deletion (with certain legal exceptions), and objection to processing. Mishandling these rights, such as failing to respond to access requests on time or refusing a legitimate deletion request, can itself be a compliance violation.

> "People want to know their personal information is safe and respected. When candidates feel in control of their data and understand how it's used, trust naturally grows in the hiring process."
>
> Serhat Elban, CEO PESCHECK

Candidate Privacy
Concerns in Hiring

Global HR systems often centralize recruitment technology, analytics, and cloud storage across regions. While this can improve efficiency, it also complicates compliance. If candidate data is stored in a non-EU jurisdiction, local laws may grant foreign authorities or service providers access rights that conflict with EU privacy standards. This creates sovereignty risks that extend beyond GDPR alone.

Key Data Points:



62% of candidates are concerned about how their personal data is managed

25% of qualified candidates disengage after a data breach

94% of candidates expect feedback after applying

62% of candidates lose interest if they don't hear back within two weeks

These figures show that privacy, transparency, and communication are closely linked. When candidates feel their data is not handled responsibly or communication is lacking, trust declines and so does engagement.

Strategic Implications for Hiring Teams

Rethinking data storage and privacy in HR is not just about compliance; it is about building trust, sustainability, and competitive advantage. Organizations that adopt data sovereignty-aware strategies benefit in several ways:

- ✓ **Improved candidate confidence**
  Transparent and localized controls reassure candidates that their data is secure and governed by familiar legal protections.
- ✓ **Reduced legal exposure**
  Minimizing risky cross-border transfers and adopting robust data governance frameworks proactively mitigate compliance threats.
- ✓ **Enhanced brand reputation**
  Demonstrating principled stewardship of personal data signals professionalism and respect for candidate rights.

In response to these trends, some HR tech vendors are launching EU sovereign cloud solutions that let organizations store and process HR data entirely within EU borders under customer control, addressing both regulatory and strategic sovereignty concerns while enabling AI integration and analytics.



Screening policy checklist

Do you want to get started with designing a screening policy? Use this checklist to keep control and an overview.

Scope and Purpose

- Define the purpose of the screening policy.
- Identify which roles require pre-employment and in-employment screening.
- Specify situations that trigger in-employment checks (promotions, secondments, client requirements).

Legal Compliance

- Ensure alignment with GDPR, local labor laws, and cross-border regulations.
- Define the types of questions and checks that are legally permissible.
- Include procedures for obtaining informed employee/candidate consent.

Types of Checks

- IIntegrity Statement
- ID Verification + Biometrics for Digital Onboarding
- Right to Work Check
- PEP, Sanction- and Watchlists Check
- Adverse Media Check
- Work-Reference-CV Check
- Qualification Verification / Diploma Check
- Credit Check
- Request of the International Criminal Records / VOG 1 2
- Upload + Validation of the International Criminal Records / VOG 3
- Address Check
- CV Cross Check

Process and Responsibilities

- Assign responsibility for screening (HR, external provider, or hybrid).
- Define steps for pre-employment and in-employment screening.
  Document how results are reviewed, interpreted, and stored securely.

Employee Communication

- Explain the purpose of screening to candidates/employees.
- Provide clear guidance on consent, privacy, and data handling.
- Identify a contact person for questions or concerns regarding screening.

Decision Making

- Define how screening results impact hiring, promotions, or assignments.
- Establish rules for handling discrepancies or negative findings.
- Ensure decisions are consistent, fair, and non-discriminatory.

Review and Updates

- Schedule periodic reviews of the policy to reflect changes in law, technology, or organizational risks.
- Update procedures for international hiring, digital checks, and emerging risk areas

Need Help or Advice in Drawing Up the Screening Policy?

Heinoud and Serhat assist many HR professionals in the background screening process on a daily basis. They are happy to share their knowledge of policy writing and implementation with you. Feel free to call us and we will gladly help you take the right steps.

Meet PESCHECK

Laying the foundation for trust

We are PESCHECK®, Europe's trusted background screening provider, with strong coverage in the Benelux and DACH regions, especially the Netherlands and Germany. Since 2015, we help organizations, from SMEs to international enterprises, make confident hiring and business decisions by combining advanced technology with local expertise.

Our approach delivers fast, reliable, and fully compliant screenings (GDPR, ISO27001, PI licensed), providing precise, actionable insights to build trust when onboarding employees, verifying partners, or safeguarding sensitive environments like high-tech, defense, finance, and consulting.

At PESCHECK, we believe trust grows through openness. Our scalable, candidate-first solutions make verification simple, secure, and efficient, turning trust into a catalyst for growth.

Schedule a meeting?

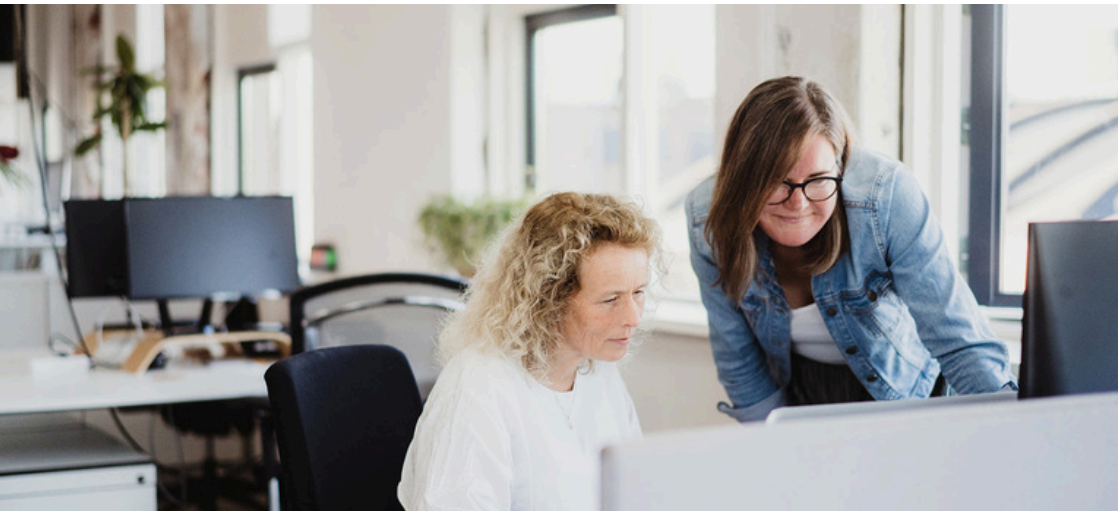
Meeting with us is always without obligation and always with the intention of helping you. Would you like to know more about drawing up a policy or conducting a background screening? Get in touch or book a convenient time directly on our website: Book a Demo.

bsi ISO/IEC 27001 Information Security Management CERTIFIED

GDPR

PBSA PROFESSIONAL BACKGROUND SCREENING ASSOCIATION

Ministerie van Justitie en Veiligheid
POB 1551



PESCHECK Definition list

Integrity Statement	9 integrity-related questions or customizable integrity statement for verification.
ID Verification + Biometrics for Digital Onboarding	Verifies the identity of a candidate using official documents and biometric data (available in 160 countries)
Right to Work	Confirms a candidate's legal right to work in a specific country by verifying work permits, visas, or residence status.
PEP, Sanction- and Watchlists Check	Cross-references candidate data against global criminal, terrorist, and law enforcement databases to assess potential risks.
Adverse Media Check	Analyzes the candidate's online footprint, including public profiles and relevant associations with keywords or reputational risks.
Work-Reference-CV Check	Verifies employment history by contacting up to 3 employers within the last 5 years, checking positions held and work performance.
Qualification Verification / Diploma Check	Verifies the candidate's highest academic qualification. Dutch diplomas are checked via DUO; international diplomas follow a broader verification process. Includes verification costs up to €25 incl. VAT (or equivalent). Any additional third-party or institutional fees may be invoiced separately, unless agreed otherwise in writing.
Credit Check	Provides a financial assessment of the candidate by checking their credit history, available in EMEA and APAC regions.

Request of the International Criminal Records / VOG 1	Requests and verifies the candidate's international criminal record or Certificate of Conduct (VOG) based on the applicable region.
Upload + Validation of the International Criminal Records / VOG 3	Facilitates the upload and automatic validation of international criminal records or VOG, ensuring compliance.
Address Check	Verifies the candidate's current or past address by cross-checking provided details with reliable or official sources.
CV Cross Check	Manually verifies the accuracy of the candidate's CV by cross-checking the details provided on the platform with the actual CV submitted by the candidate.

pescheck

Trust grows in the light of openness

pescheck

Headquarters
Capitool 10, 7521 PL
Enschede, Netherlands
(0)85 060 8999

Germany Office
Franz-Joseph-Str. 11
80801 Munich
Bavaria, Germany

Follow Us
X
Facebook
LinkedIn