Background Screening Advancements in Deutschland, A Screeners Perspective.

Bon Idziak

Chief Compliance Officer

ACCURATE Background, Inc.

Disclaimer

The material discussed during this discussion should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

20 year industry professional and subject matter expert on the topics of Background Screening and HR Technology

- Executive Committee, Board of Directors for the National Association of Professional Background Screeners (NAPBS)
- President/Chairman, Board of Directors for the HR Open Standards Consortium (Worldwide)
- Board of Directors and President for The Sue Weaver C.A.U.S.E., (Consumer Awareness of Unsafe Service Employment) a 501 (c)(3) non-profit, founded in 2004 to promote workforce screening for in home-service providers

A discussion on the advancements to the Background Screening of Employees in Deutschland with Data Privacy Protections related to EU Privacy Shield and GDPR for companies operating globally.

Typical Background Check

Typical Background Checks include:

- Education Check (highest level)
- Employment Check (most recent)
- Professional License
- Professional Reference
- ID Check

Less Common Checks

- Address Check
- Relevancy
  - Credit Check
  - Driving Record
- Executive
  - Media Check
  - Civil Litigation
  - Directorship

Q: Are Criminal Records Checks

More Common

or

Less Common

Criminal Record Checks in Germany

Q: Can an employer conduct a criminal record search on a candidate employee in Germany?

A: The starting position is that the employer should not, as a general rule, conduct criminal record searches on candidates/employees in Germany.

- (i) there must be a legitimate interest justifying the criminal record information request; and
- (ii) the information request must cover relevant criminal history only.

Q: Can a “certificate” of clearance be requested from the candidate by an employer?

A: Yes, if the employer has a legitimate reason for making the request, they can ask the candidate to provide information in respect of their criminal record in the form of a certificate.

Only the employer may ask the candidate and only the candidate can provide the certificate (which may be provided to a third-party).

Residents

You can apply for a Certificate of Conduct (Führungszeugnis) in person at your local registration office (Meldebehörde) in which you are currently registered or you can apply online on the website of the Federal Office of Justice if you have a valid and recognized electronic signature (elektronischen Personalausweis) such as an electronic residency permit (elektronischen Aufenthaltstitel) and a card-reading machine (Kartenlesegerät).

Non-Residents

Information for applying for a certificate of conduct for persons living outside the Federal Republic of Germany

- Sending your application to the Federal Office of Justice located at:
  - Bundesamt für Justiz
  - Referat IV 2
  - 53094 Bonn
- Apply in person directly in Germany at the Federal Office of Justice located at:
  - Bundesamt für Justiz
  - Besucherservice
  - Adenauerallee 99 - 103
  - 53113 Bonn

Non-Residents

If your certificate contains entries and you are a Non-Resident, the Federal Office of Justice will forward your police certificate to the German embassy or consulate where you reside and you will be invited to come and look at the document in person. In order for the German embassy/consulate to send this document to anyone else, you must give your consent.

Comparison to US

Federal Law (Fair Credit Reporting Act or FCRA)

- Disclosure
- Authorization
- Pre-Adverse Action Notice
  - Dispute and Reinvestigation
- Adverse Action Notice

- Equal Employment Opportunity Commission *GUIDANCE*

Privacy Shield

GDPR

Data Protection Standards

Privacy Shield

Notice –inform candidates of the 'what, why, how, when and where' of data collection

Choice –provide candidates with opt-out and opt-in options when we share personal data with 3rd parties for a purpose different than that originally authorized by the candidate (e.g. this would apply if we wanted to share candidate data with a third party for marketing purposes, which we do not do).

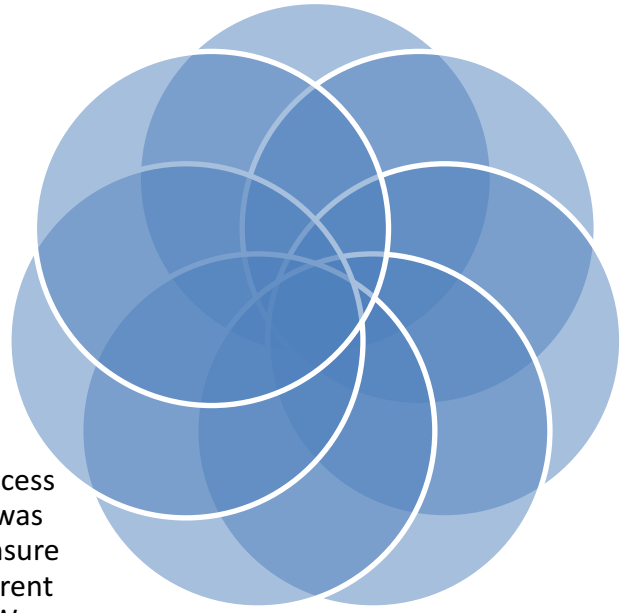
Onward Transfer –ensure that any vendors or subcontractors that will have access to EU candidate data will only be provided that data for the purpose authorized by the candidate and that such parties will be obligated to the Privacy Shield principles.

Security –take reasonable and appropriate measures to protect personal data from loss, misuse, and destruction.

Data integrity –only collect and process data for the purposes for which it was authorized by the candidate, and ensure that data is accurate, complete, current and reliable for its intended use. We may not retain data for any longer than necessary to serve a purpose of processing.

Access –provide access, upon a candidate's request, to the data maintained about him or her and give the candidate the opportunity to correct, amend, or delete information if it's inaccurate or incomplete.

Enforcement – we ensure that the privacy principles are complied with.



ACCURATE Background, Inc.

GDPR

- The GDPR is Europe's new data protection law. It governs the protection of personal information of individuals located in Europe (regardless of residence or nationality – this means that if a person is a citizen of the EU with a place of residence in the EU, they will not be protected by the GPDR once they are outside the EU.) **It is effective 25 May 2018.**
- Europe has had a Data Protection Directive in place since 1995 – it was out of date and had to be "implemented" in each EU member state via separate legislation (e.g. the UK Data Protection Act 1998) which led to some divergence of interpretation.
- The GDPR is different because it carries the force of law throughout Europe and EU member states will not necessarily be required to create separate enforcing legislation (although they may supplement the GDPR to a certain extent).

Data Privacy

Several factors are combining to make the issue of data privacy important for the transfer of HR information.

- The recent European court decision invalidating Safe Harbor and the EU/US response of introducing the EU-U.S. Privacy Shield has brought forward the issue of cross-border transfers and sending data from Europe to the US.
- The forthcoming General Data Protection Regulation (GDPR) which comes into effect in 2018 widens the scope of European data protection legislation and clarifies that organizations must delete personal data after it is no longer needed.
- Data protection laws in Russia and other countries which impose geographical restrictions on data make it desirable to tag data with which countries it is allowed to do.
- The prevalence of data breaches makes most corporations very careful about where their employee data can go and how sub-processors can process them.

- HR Open Standards recommends using the Data Privacy schema to allow organizations passing Personally Identifiable Information (PII) data to a third party to add data privacy requirements.

- The Common/json/base/DataProtectionPolicyType includes simple metadata to attach to data in the context of HR (employee) data. This recommendation does not attempt to suggest metadata for every use case, however, it does provide a minimal set of useful metadata. Refer to the Implementation Guidelines within each domain for use cases and sample data.

1. Retention Date

To conform with regulatory requirements related to PII retention it would be helpful to associate a retention date with PII data. This would help organizations comply with the GDPR requirement that give organizations “the obligation to erase personal data without undue delay … where … personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed”.

- May be kept indefinitely
- May be kept until 'date' after which must be deleted
- May be kept for NN number of days

2. Geographical Restrictions for Storage

To conform with regulatory requirements related to where data is and isn't allowed to be stored it would be helpful to have a tag to specify geographic restrictions. This would help organizations comply with various requirements including the European restrictions on data leaving Europe, Russian regulations on data leaving Russia and some US organizations who prefer to have data remain in the US.

- No geographical restriction
- Must remain in the specified country
- Must remain in specified countries

3. Geographical Restrictions for View and Edit

To conform with regulatory requirements related to where data is and isn't allowed to be viewed and changed it would be helpful to have a tag to specify geographic restrictions. This would help organizations comply with various requirements on where data might be viewed or edited.

- No geographical restriction
- May only be viewed and edited in the specified country
- May only be viewed and edited in the specified countries

Meta Data Use Case

When there is an exchange of data between two systems that involve PII, and there is a jurisdictional requirement (such as data crossing an international border), then the producing system should indicate the restriction.

Colin Grange has just graduated from high school. He registers as unemployed with the local PES office in Sweden by using an on-line registration application. He chooses to send his information to 3 of the career sites that reside in different countries. The PES system then sends the updated information to the chosen sites. To conform to data protection rules in the affected countries (Denmark, Norway, and Finland) of the chosen career sites, and the wishes of the person, the data retention rules are communicated by the PES System.

Sample JSON Instance of Use Case

Below is a snippet of the sample JSON instance to go with the above use case:


```
{
   "documentId": {
      "value": "Candidate061",
      "schemeId": "PESSweden"
   },
    "dataProtectionPolicy": {
      "retentionDate": "2017-04-30",
      "retentionDays": 365,
      "geoRestrictions": [{ "country": "NO", "policy": "Read" },
                  { "country": "DK", "policy": "Read" },
                  { "country": "FI", "policy": "Read" }]
   },
   "uri": "https://hr-xml.org/lightweight_recruiting_example/getCandidate/61",
   "person": {
      "name": {
         "formattedName": "Colin Grange",
         "given": "Colin",
         "family": "Grange",
         "preferredSalutationCode": "Mr."
      },
      "height": {
         "value": 180,
         "unitCode": "CMT"
      },
      "weight": {
         "value": 80,
         "unitCode": "KGM"
      },
      "gender": "male",
      "birthDate": "1998-03-26”,
```


ACCURATE Background, Inc.

Contact Me

Thank you!

Bon Idziak

bidziak@accuratebackground.com

ACCURATE Background, Inc.