



Summary

1 Introduction and reason for the study

The public accessibility of personal data in public records is under increasing pressure in the digital age. Whereas physical accessibility to information used to provide natural protection, developments in digitalisation, automation and artificial intelligence have largely removed these barriers, making personal data easier to collect, combine and reuse.

Public registers defined as registers established by or under the law, and accessible to anyone (i.e. regardless of your capacity or interest), perform important societal functions, such as ensuring legal certainty, transparency of administration, and protection of economic interests. However, increased accessibility creates tension between this public accessibility and the fundamental right to data protection.

This tension has been further exacerbated by rulings by the EU Court of Justice, including drawing a line under the public nature of the UBO register, and concerns raised by the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) and register administrators about abuse risks ranging from identity fraud to harassment.

In response to these concerns, the Research and Data Centre (*Wetenschappelijk Onderzoek- en Datacentrum*, WODC) commissioned this study (project number 3457). The aim was to test the public accessibility of personal data in 13 specific public registers against European data protection law and to identify privacy-protecting measures that could bring these registers into compliance where needed or future-proof them in light of technological developments.

2 Research question and methodology

The central question in this study is:

Is the public accessibility of personal data in the public registers under investigation in line with data protection law? And what privacy protection measures are needed to bring and/or keep these registers in compliance?

To answer, we have developed an assessment framework based on case law and relevant regulations, consisting of four key questions:

1. **Foreseeability and predictability:** Is there a clear legal basis for the public disclosure?
2. **Objective and appropriateness:** Does the register meet the objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others and is publicity an appropriate means to achieve these objectives?
3. **Subsidiarity:** Are less intrusive alternatives possible?
4. **Proportionality:** Is practical accessibility proportionate and are there sufficient safeguards?

The research approach combines legal-dogmatic research with practice-oriented methods. For each register, interviews were conducted with administrators, desk research was carried out, and quantitative data on use and access were collected and analysed where possible. The research was guided by a supervisory committee to ensure scientific quality, among other things.

3 Main findings from the study

After analysing the 13 registers examined, it can be concluded that two of the 13 registers should not be public at all.

In the case of the List of licence holders Private Security Organisations and Detective Agencies Act (*Register vergunninghouders Wpbr*), the legal basis for the public nature of the register as a whole is lacking, and in the case of the Parental Authority Register (*Centraal gezagsregister*), the legal basis is there, but the study shows that it is not sufficiently demonstrated that making the register public can contribute to achieving the purpose of the register. In addition, it has not been demonstrated why public access in this case may be considered a subsidiary measure and why limited access for pre-defined groups with a demonstrable interest could not be used. Given the fact that this register contains personal data of both parents and children, wide access is disproportionate because of the inherent security risks for this vulnerable group.

The remaining 11 registers largely meet the requirements of data protection law for public disclosure, but fall (seriously) short in some respects. **Seven of the 11 remaining registers lack a basis for the disclosure of one or more personal data contained in the register.** All four registers examined within the Central Insolvency Register (bankruptcy, suspension of payments, debt rescheduling scheme for natural persons (WSNP), and the Dutch Scheme of Arrangement (WHOA)) lack a legal basis for the publication of certain personal data. For the WHOA, this concerns very limited and not particularly sensitive data. However, both the bankruptcy (*faillissement*) and suspension of payments (*surseance van betaling*) registers involve the publication of bankruptcy reports, which can be full of personal data, including of a more sensitive nature. The WSNP register also lacks the basis for publication of place of birth and residential address in some cases. For the Central Guardianship and Administration



Register (*Centraal curatele- en bewindregister*), the basis for publication of place of birth is also lacking. The Register of sworn interpreters and translators (*Register beëdigde tolken en vertalers*) seems to lack a linking provision, as a result of which the publication of data on the so-called fallback list (*uitwijklijst*) is not lawful. This while disclosure does seem to be the intention and does happen in practice.

In all 11 of these remaining registers, shortcomings in privacy protection measures were found, even though they largely comply with disclosure requirements. These include the overall lack of adequate logging of who accesses the register, as well as some specific areas of concern, such as poor technical safeguards against bulk access, inconsistent access procedures between courts, inclusion of unnecessary data such as salutation or place of birth, unclear user groups, and confusion about giving consent for public disclosure of some personal data where it is actually mandatory and not a choice.

4 Assessment results by register

List of licence holders Private Security Organisations and Detective Agencies Act (*Lijst vergunninghouders Wet particuliere beveiligingsorganisaties en recherchebureaus*)

Purpose and function: This register contains the names of organisations licensed to act as private security organisations or detective agencies. It is intended to inform third parties about the licensing status of these companies.

Conclusion: Not compliant with data protection law.

Key problem: There is no legal basis for the disclosure of information in the register. Although the register contains only company names, many of them contain personal data, and whether or not a company is licensed also says something about the natural person behind the company in certain circumstances. The register therefore also discloses personal data. The basis is currently being worked on, but does not yet exist.

The register fulfils a practical need in the market. Once a sound legal basis is realised, we additionally recommend the following improvements.

Recommendations:

- Restrict the accessibility of the registry by not allowing bulk transfers by default, unless there is a separate and explicit justification for this which is reflected in the in the legal basis created in national law or the explanation thereto.
- Delete outdated pdf lists still available on the website.
- Formulate a unified policy on whether or not to include address information.

**Netherlands Register of Court Experts
 (Nederlands Register Gerechtelijk Deskundigen, NRGD)**

Purpose and function: The NRGD is a quality register that includes forensic experts who meet established standards. Criminal justice chain partners, such as the Public Prosecution Service and the judiciary, are often obliged to use experts from this register.

Conclusion: The NRGD is in line with data protection law, but there are some concerns.

Key points: The legal basis is clear and the data disclosed are limited in nature. Furthermore, the NRGD has properly implemented the principle of data minimisation when it comes to the indication of the expert's gender: this is *only* displayed for a category of experts where it is relevant.

Point of note: Experts supposedly 'consent' to disclosure when registering, whereas it is mandatory. This may create confusion about its voluntariness.

Recommendation: Delete disguised consent to disclosure. Replace this with clear wording on the consequences of recording certain data. In other words, inform the experts rather than ask for their consent.

**Central Insolvency Register – Bankruptcies
 (Centraal Insolventieregister – Faillissementen)**

Purpose and function: The register informs the public about bankruptcy proceedings and relevant steps taken during the proceedings, with the aim of ensuring transparency for debtors and facilitating economic activity in general.

Conclusion: The CIR - Bankruptcy partially violates data protection law.



Key points:

- There is no legal basis for publishing bankruptcy reports.
- For natural persons (without a company), the publication of residential address and date of birth, among others, may be disproportionate.
- Information is published in both the CIR and the Official Journal (*Staatsblad*), with no clear justification for this duplication.

Recommendations:

- Suspend publication of bankruptcy reports until a legal basis is achieved.
- Stop publishing personal data such as date/place of birth and residential address until an adequate legal basis is provided.
- Further research should be carried out on the need to publish personal data in the Official Journal, with particular attention to cases of publication concerning natural persons who have been declared bankrupt.
- The registration and use of date/place of birth and residential address can be retained and used as a verification question. However, these data do not *all* have to be subsequently shown in the registration, in particular the address can be omitted here.

Central Insolvency Register - Suspension of payments

(*Centraal Insolventieregister – Surseance van betaling*)

Purpose and function: This register contains information on moratorium proceedings, in which an entrepreneur is granted a suspension of payments under the supervision of an administrator. Its purpose is to inform creditors and other stakeholders about the status and progress of the proceedings.

Conclusion: The CIR - Surseance partly violates data protection law.

Key points:

- There is no legal basis for publishing suspension reports.
- In the case of natural persons (with a company), personal data is disclosed - such as home address and date of birth - while its proportionality is debatable.
- Again, double publication takes place in the CIR as well as the Official Journal, without substantiation of necessity.

Recommendations:

- Cease publication of suspension reports while there is no legal basis for it.
- Delete the publication of specific personal data such as date of birth and residential address unless there is an explicit and sufficient legal basis for doing so.
- Limit the disclosure of the residential address of natural persons unless it is also the official mailing address.
- Offer natural persons who conduct their business from home the opportunity to register an alternative postal address.
- Conduct a study on the need for dual publication in the Official Journal and the CIR, paying particular attention to the position of natural persons.

Central Insolvency Register - WSNP (Natural Persons Debt Rescheduling Act)
(Centraal Insolventieregister – WSNP (Wet schuldsanering natuurlijke personen))

Purpose and function: This register contains details of persons admitted to the statutory debt restructuring process. Public access to the register is intended to inform creditors and other interested parties of the status of these proceedings.

Conclusion: The CIR - WSNP partially violates data protection law.

Key point: The disclosure of personal data of natural persons participating in WSNP proceedings lacks a clear need in some cases.

Recommendations:

- Delete the standard disclosure of the place of birth and residential address of natural persons. Their registration can be maintained and also used for the purpose of locating the specific natural person, but these details need not be shown when the register is consulted.
- A further study should be carried out on the need to publish personal data in the Official Gazette, with a particular focus on debt restructuring cases.

Central Insolvency Register - WHOA (Dutch Scheme of Arrangement Act)
Centraal Insolventieregister – WHOA (Wet homologatie onderhands akkoord)

Purpose and function: The WHOA proceedings offer companies in financial difficulties, including natural persons exercising a self-employed profession or business, the possibility of reaching an agreement with creditors outside



bankruptcy. The Central Insolvency Register makes reports on public WHOA proceedings transparent, including to creditors, courts, and market participants.

Conclusion: The CIR - WHOA is broadly in line with data protection law, with some necessary areas of improvement.

Key problem: To date, only data on legal persons, such as BVs and NVs, have been published. This limits most privacy risks. However, within the register, personal data of officers such as the observer and expert are also published (including name, address and phone number), without an explicit legal basis.

In addition, the entire WHOA register is accessible without barriers via a central website, without the use of verification questions or access limits. This allows for bulk access and puts pressure on the proportionality of disclosure, especially if natural persons (practising a self-employed profession or business) will eventually be covered by the proceedings

Recommendation: Make provisions in case the WHOA will include natural persons acting in a self-employed profession or business with regard to accessibility. Do not make the register accessible in its entirety via the website, but introduce a search functionality, equipped with the necessary safeguards to prevent bulk, or multiple occasional, disclosures.

Matrimonial property register (*Huwelijksgoederenregister, HGR*)

Purpose and function: This register contains information on prenuptial agreements, property separations, and other agreements affecting the property of (former) partners. The register serves two purposes: it enables spouses to disclose their matrimonial property situation to third parties, and protects third parties from the consequences of unregistered prenuptial agreements. Registration is not mandatory, but without registration, prenuptial agreements cannot be invoked against unknowing third parties.

Conclusion: The matrimonial property register is broadly compliant with data protection law, but its effectiveness is under pressure.

Key points:

- The disclosure itself is subject to conditions: to access the register, the surnames of both partners as well as the date of marriage or registered partnership must be entered. This verification constitutes an important privacy protection measure. At the same time, there is criticism in the

literature that this very requirement creates too high a threshold, resulting in insufficient consultation of the register.

- It is also unclear who actually consults the register: around 490,000 requests were registered in 2023, but due to the lack of user information, it cannot be determined whether this comes from a broad target group or largely from professionals such as notaries.
- Furthermore, the register only provides notice that prenuptial agreements have been registered; the content is only accessible to a limited group (such as the parties involved, notaries and certain authorities). The question has been raised whether this limited access fulfills the legal intentions and whether this working method, introduced in view of the GDPR, further hinders the effectiveness of the register.

Recommendation: Implement a system where it will be possible to distinguish categories of consulters of the register, on the basis of which the effectiveness of the register can start to be measured.

Estate register (*Boedelregister*)

Purpose and function: The estate register contains information on estate dispositions and estates. The register aims to provide interested parties, such as heirs, notaries or creditors, with insight into current estate proceedings. The registers are held decentrally at the registries of the courts.

Conclusion: The openness of personal data in the estate register largely complies with data protection law. However, the method of accessing the register does not fully align with legal requirements and lacks uniformity between courts.

Key point: There are differences in practices among the various court registries, not all of which are in line with the law. For example, the Amsterdam District Court incorrectly requires a copy of an identity document when requesting information, and the North-Holland District Court asks for the reason for consultation. Both practices are not in line with Article 7 of the Estate Register Decree and may have a deterrent effect, including on legitimate consulters of the register.

Point of attention: Limited accessibility is an effective safeguard, but also a practical barrier. For ease of use (and consistency with other registers), digitisation could be considered, subject to strict conditions.



Recommendations:

- The requirement of a copy of identity proof by the Amsterdam District Court before the register can be accessed should be scrapped immediately.
- The request for reasons for the application by the North Holland District Court should be stopped immediately.
- Consider regulating the estate register at the national level in a manner similar to the matrimonial property register, in the form of a referral index.
- Ensure a uniform method of consultation across courts and its requirements. In doing so, evaluate whether the current verification questions are really necessary or whether they create an unreasonable barrier for legitimate stakeholders who wish to access the register.

Parental Authority Register (Centraal Gezagsregister, CGR)

Purpose and function: The CGR is a public register in which legal facts are recorded regarding the custody of minors in cases where custody does not follow by operation of law, such as joint custody declarations by unmarried parents or the appointment of a guardian. The register serves to give third parties insight into who is legally authorised to act on behalf of a child, for example in situations involving passport applications, medical decisions or in establishing (vicarious) liability.

Conclusion: The Parental Authority Register does not comply with data protection law.

Key points: The broad disclosure of the CGR is insufficiently substantiated, especially given the sensitive nature of the data on minors. Current custody relationships can only be inferred indirectly, limiting the effectiveness of the register. Post-death guardianship appointments are disclosed prematurely, and access procedures vary from court to court. All this raises serious questions of proportionality, subsidiarity and effectiveness of the register.

Recommendations:

- Delete the public nature of the Central Authority Register and make the register accessible only to persons with a demonstrable legitimate interest. Draw up an exhaustive list of parties for whom such an interest may be presumed.
- Delete immediate disclosure of post-death guardianship appointments. Make this information public only when it becomes legally relevant.

Register of sworn interpreters and translators (Register beëdigde tolken en vertalers, Wbtv-register)

Purpose and function: This register contains details of sworn interpreters and translators and is designed to enable chain partners such as the police, the judiciary, and lawyers to quickly find authorised professionals.

Conclusion: The Wbtv register is broadly compliant with data protection law, with some areas for improvement.

Key points: There is no formal basis for departing from legal publication requirements as set out in the Wbtv, despite applying data minimisation. The possibility of voluntary disclosure of additional personal data is legally vulnerable, as professional registration is mandatory. Furthermore, technical measures such as logging and access control are lacking, so misuse cannot be excluded or detected.

Recommendations:

- Utilise the legal possibility to shield data via a governmental decree (amvb) that is currently not publicly disclosed.
- Consider making it explicitly clear, through an additional link clause, that the specific rules in the Sworn Interpreters and Translators Decree (*Besluit beëdigde tolken en vertalers*), especially Article 10, regarding the nature and scope of personal data that may be included and disclosed, apply not only to the main register, but also to the Fallback List (*Uitwijklijst*).

Central Guardianship and Administration Register (Centraal Curatele en Bewindregister, CCBR)

Purpose and function: The CCBR provides insight into the legal capacity and power of representation of persons placed under guardianship or administration, and also lists who has been appointed as guardian or administrator. The register aims to prevent debt problems and legal uncertainty for third parties.

Conclusion: The CCBR is broadly in line with data protection law, with one explicit shortcoming and some areas for improvement.

Key points: The disclosure of the data subject's place of birth has no legal basis and is therefore not compatible with the GDPR. In addition, the contractual retention periods for Webservice customers are relatively long, and the general



terms and conditions of that Webservice do not apply to guardianships. Finally, there is no explicit legal justification for processing special personal data in the case of guardianship.

Recommendations:

- Delete disclosure of birthplace in CCBP.
- Adjust the terms and conditions of the Web service to include protective custody.
- Shorten the contractual retention period for recipients of data from the register after the termination of guardianship or administration.
- Record explicitly that the processing prohibition of Article 9(1) GDPR on special categories of personal data, such as health data, is broken by virtue of Article 9(2)(g) GDPR jo. art. 1:391 BW.

**Ancillary relationships register judicial organisation
(*Nevenbetrekkingsregister rechterlijke organisatie – NERO (judges)*)**

Purpose and function: The NERO register provides insight into ancillary relationships of judges, with the aim of ensuring independence, impartiality and transparency within the judiciary. Disclosure is legally enshrined in the Wvra.

Conclusion: NERO is in line with data protection law, with some technical and substantive concerns.

Key points: Accessibility is too broad: the register is searchable in bulk without restrictions, which increases the risk of misuse. In addition, the added value of stating salutation (mw./dhr.) is insufficiently substantiated.

Recommendations:

- Limit bulk search possibilities by requiring targeted searches by name, with some margin of error allowed. Exclude searching only by function or court. However, this may be used as a (non-mandatory) verification question.
- Delete the salutation (mw./dhr.) unless a functional purpose can be demonstrated.

**External relations register public prosecutor's office
(*Nevenbetrekkingenregister openbaar ministerie – NEOM (members of the public prosecutor's office)*)**

Purpose and function: The NEOM register is intended to provide insight into ancillary relationships of members of the public prosecutor's office, to support transparency and confidence in the independence of the Public Prosecution Service (Openbaar Ministerie). The public nature of the register also follows from the Wrra.

Conclusion: NEOM is not fully compliant with data protection law. The legal basis is in place, but the technical implementation and degree of substantive openness undermine the purpose of the registry.

Key points: Many ancillary functions are described in vague, generic terms. Location details are often missing. Moreover, a technical character limit restricts the display of complete job descriptions. At the same time, there is also unlimited searchability, which increases the risk of misuse.

Recommendations:

- Require full and specific description of ancillary relationships and organisations involved, unless there are concrete security risks that justify a more restrained presentation.
- Lift the technical restriction on the number of characters displayed in the registry entry.
- Delete the salutation (mw./mevr. and dhr).
- Limit bulk search possibilities by requiring targeted searches by name, with some margin of error allowed. Exclude searching only by function or court. However, this may be used as a (non-mandatory) verification question.

5 Conclusion and recommendations

This study shows that of the 13 registers examined, two should not be public at all: the List of licence holders Private Security Organisations and Detective Agencies Act because of the lack of a legal basis, and the Parental Authority Register because its wide accessibility is insufficiently substantiated and poses disproportionate security risks for minors. Of the remaining 11 registers, seven lack a basis for the disclosure of certain personal data, while all 11 have shortcomings in privacy protection measures.

The public accessibility of personal data in registers remains justified only with greater attention to actual use and practical accessibility. Technological developments make personal data from public sources increasingly vulnerable to improper use. The



problem has become primarily a question of accessibility, not just the public nature of the register. Where practical barriers once provided natural protection, data can now be easily collected and combined en masse.

The study identifies four categories of structural challenges: legal foundations, data-oriented challenges such as lack of data minimisation measures taken and bulk access risks, process-oriented challenges such as inadequate monitoring of actual use, and lastly the need for further examination of dual publication in both registries and the Official Journal. Future-proof registries require regular evaluation and updating, legally, technically, and organisationally. Without adequate insight into who consults the registers, it remains difficult to assess effectiveness and proportionality.

Based on this research, we make the following recommendations, grouped into four main categories:

Legal measures:

- Provide explicit legal bases for all disclosed personal data for which disclosure is deemed necessary.

Data-driven measures:¹

- Implement layered access where possible, with basic information widely accessible and limit access to detailed information.
- Prevent bulk requests by requiring targeted searches and introducing a standard procedure for legitimate bulk requests.
- Limit the default display of personal data to what is strictly necessary.
- Harmonise verification questions in decentralised registers such as the estate register.

Process-oriented measures:²

- Implement standard protection measures, such as rate-limiting and robots.txt.
- Provide systematic logging and monitoring to analyse usage patterns.
- Develop uniform guidelines for shielding personal data in extraordinary situations.

¹ This follows the categorisation set out in the Ministry of Justice and Security's 2023 *Privacy by Design Manual*, now that government bodies are already familiar with it. These include the following: 'The data-oriented strategies focus on the processing of personal data itself and are therefore technical in nature. The data-oriented strategies are mainly concerned with technical aspects of processing personal data' (Bennink & Drukarch 2023, p. 10). Translation by the authors.

² 'The process-oriented strategies are organisational measures. These measures focus on the organisation and the people within it rather than the technical measures that can be taken, e.g. providing information to data subjects' (Bennink & Drukarch 2023, p. 11). Translation by the authors.

- Periodically evaluate the effectiveness of registries and their use by intended target groups.
- Facilitate easy access for easily identifiable target groups, such as government agencies and professional groups.

Further research

- Conduct further investigation into the need for publication of personal data in the Official Journal.

The recommendations offered in this report are a necessary starting point for addressing the identified bottlenecks. Swift implementation is essential to mitigate privacy risks without compromising the social value of these registries, ensuring both legality and effectiveness now and in the future.