Necessary Processing of Personal Data: The Need-to-Know Principle and Processing Data from the New German Identity Card

Harald Zwingelberg

Necessary processing of personal data: the need-to-know principle and processing data from the new German identity card

Harald Zwingelberg[1]

[1] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Holstenstr. 98, 24103 Kiel, Germany, hzwingelberg@datenschutzzentrum.de

Abstract. The new German electronic identity card will allow service providers to access personal data stored on the card. This imposes a new quality of data processing as these data have been governmentally verified. According to European privacy legislation any data processing must be justified in the sense that the personal data are necessary for the stipulated purpose. This need-to-know principle is a legal requirement for accessing the data stored on the eID card. This text suggests a model as basis for deriving general guidelines and aids further discussion on the question whether collecting personal data is necessary for certain business cases. Beyond the scope of the German eID card the extent and boundaries of what can be accepted as necessary data processing poses questions on a European level as well.[1]

Keywords: Necessary data processing, identity management, anonymous authentication, German electronic identity card, neuer Personalausweis.

1 Introduction

Since November 2010 a new German identity card, called “neuer Personalausweis” (nPA) is being rolled out. The nPA promises new functionalities allowing the holder to securely and trustworthily identify herself online. Security is meant in relation to the underlying technology. Trustworthiness refers to the identifying information on the nPA which are verified by governmental bodies.
The legal regulation on which the nPA is based took into account the protection of the holder’s privacy and enacted the requirements following from the European legal framework. The purpose binding principle is reflected by the law which requires that data collected from the nPA must be necessary for a previously specified and legally allowed purpose, § 21 sec. 2 PAuswG.[2] Generally only the minimum data required for

[1] The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216483 for the project PrimeLife.

[2] Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAuswG = German Law on Identity Cards), available online:

the stated purpose may be collected [1, p. 14]. As further details on which personal data may be deemed necessary are missing in the law, this assessment is left to (1) legal practitioners at the Bundesverwaltungsamt (BVA), a German federal authority issuing the permit to access the data, (2) the data protection authorities supervising the use of access credentials and, eventually, (3) courts in case they become involved. The law provides for a final control of the holder prior to a transmission of any data from the nPA to data controllers. Contrary to other European eID solutions, the German solution employs a double-sided authentication [2, p. 4] requiring data controllers to transparently display their identity prior to any collection of personal data from the nPA. This requirement is enforced as access to data on the nPA is possible for third parties only when they present a valid access certificate containing their own identity to the holder of the nPA [3, p. 43; below section 2.1].

Governmental eIDs such as the German nPA also introduce a new level of privacy-related issues: The personal data stored on the card have been proven and confirmed by a governmental authority. This provides a higher level of certainty for parties relying on the information and a safeguard against identity fraud. However, the use of such accurate data may have privacy-infringing aspects as well because it may become harder or even impossible for users to employ services anonymously or pseudonymously. It thereby contravenes basic concepts of modern privacy-enhancing identity management systems [4, p. 16]. While integrity of identifying information is valued and necessary in many business transactions, it would highly compromise privacy if personal information was always provably correct. In such a scenario humans were incapable to plausibly deny anything logged by a machine. In consequence information technology could take over control over personal privacy [cf. 5]. Therefore a balance between integrity of information required for trusted transactions and deniability preserving privacy was sought by the legislator and found by allowing the use of verified information only where necessary for the legitimate purpose at hand. Additional policy-related requirements in this respect are the principles of data minimization and purpose limitation that both may be derived from existing European and Member States' privacy legislation [1, p. 14][6 at para. 2.30, 2.89]. Applying these principles to the nPA, the German law requires a governmental proof that the personal data transferred to a third party are actually necessary for the transaction in question. This proof must be provided in form of an access certificate.

---

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/eperso.pdf?__blob=publicationFile.

Necessity for processing of personal data / necessary data processing: According the German law, accessing personal data on the nPA is only allowed if it is necessary for a legally allowed purpose. This paper analyzes common use cases for the deployment of the nPA. It aims to identify general guidelines for the assessment whether the data processing is necessary.[3] Such evaluation of the necessity will be done by the German authorities prior to allowing access to data stored on the nPA.

The **holder** of an nPA is the customer or citizen involved in a transaction with the need to identify or authenticate himself towards a service provider or, in case of citizens, towards a public authority. The **service provider** offers any kind of service or goods. For the nPA, the German government acts as identity provider administering the personal data stored on the nPA.

2 Regulatory framework

The German regulatory framework for processing personal data in connection with the nPA is strongly influenced by the European Privacy Directives, namely the Data Protection Directive 95/46/EC (DPD) and the Directive on Privacy and Electronic Communications 2002/58/EC (e-Privacy Directive). The Directive 2009/136/EC amending directive 2002/58/EC has not been transposed into German law yet.

2.1 The German Personalausweisgesetz

The legal basis for data processing with the nPA is the German Personalausweisgesetz (PAuswG) passed in June 2009. The nPA contains a chip which stores certain personal data on its holder. The data available for the identification service comprises: lock flag, expiry date, family name, given name, doctoral degree, date of birth, place of birth, address, type of document, service-specific pseudonym, abbreviation "D" for Germany, information whether the holder is older or younger than a given age, information whether the place of residence is identical to a given place, and a stage name for artists. This exclusive list is provided in § 18 sec. 3 PAuswG. Additional personal data such the holder's picture or fingerprints are reserved for use by certain authorities with the right to identify persons (police, customs, tax fraud investigation and border police) [7, p. 672 et seq.]. These biometric data will not be available as part of the eID function and are therefore not part of this analysis.

[3] To the best knowledge of the author there had been no generic analysis of the requirement of necessity beyond the scope of individual cases [e.g. 10 at § 28 BDSG para. 14 et seq. with further references]. However, requirements for a web shop scenario had been analyzed within the Project PrimeLife[3] in the context of developing a privacy compliant web shop frontend for collecting user data [9]. In regard to use of personal data retrieved from the nPA only the explanatory statements from the legislative process [3] are currently available. Based on the research leading to this paper an ad hoc working party of the German data protection authorities published guidelines for the access to data on the nPA [8].

The personal data will be transmitted only when the service provider has shown the holder of the nPA an access certificate indicating the service provider's identity, the categories of personal data to be transmitted, the purpose of the planned data processing, the address of the data protection authority in charge and the expiry date of the certificate, § 18 sec. 4 PAuswG. Prior to the actual transmission the holder has to give consent to the request which is displayed together with the access certificate in the software to be used with the nPA (called AusweisApp). At this stage she is enabled to deselect some of the information which will then not be transmitted to the service provider. This provides a certain extent of user control over the data transmission. For enhanced transparency every data transmission could be stored in a protocol file also including information about the receiving service provider. This protocol should be stored on the local machine under the user's control. Whether such a feature will be part of the official software is unknown to the author but certainly it is advisable to keep such a protocol.

Attaining an access certificate is a two-step process.[4] To attain an access certificate, a service provider must first apply for an authorization issued by the BVA. At this step the BVA checks whether the purpose of the data processing is not violating the law and that the personal data is actually required for the stipulated purpose, § 21 sec. 2 no. 1 and no. 2 PAuswG. Authorizations are valid for a period up to three years. Access certificates issued on the basis of the authorizations by privately owned trust centers allow multiple accesses for the purposes fixed in the authorization and named in the certificate. This paper will identify patterns and develop guidelines for the question whether certain personal data are necessary for a given type of use case, e.g., a certain business or governmental process.

2.2 Staged approach

The system set forth by the PAuswG allows practically for three legal consequences: denial of access to the personal data stored on the nPA, disclosure only of the pseudonym or derived information, e.g., being over 18 years of age, or allowing access to those personal data necessary for the purpose at hand. The analysis done on basis of use cases provided a bigger picture showing that the amount of necessary data processing correlates with stages of typical contract negotiations. Another result of the analysis had been that besides the stage of the negotiations also other factors such as the chosen payment method are of major relevance. As the model helps to identify such issues this approach has been suggested for the assessment of the necessity of data requested by service providers when applying for an authorization at the BVA [8]. The staged model could also provide a basis for future discussion on the assessment of which processing of personal data can be deemed necessary. A better understanding of what processing is necessary will be useful for the development of privacy enhancing technologies such as automated matching and negotiating of user's privacy preferences with a service provider's privacy preferences [cf. 9].

[4] Data controllers will also have to proof secure data processing in a separate process. However, here only the legal requirements are mentioned as requirements in respect to technical and organizational measures are beyond the scope of this contribution.

In Stage 1 the holder only seeks information about a service. At this stage processing of personal data is usually not necessary. Rather the services should allow the holder to access the information anonymously or under pseudonym. This is also in conformity with European privacy legislation, [cf. recital 9 of the e-Privacy Directive]. Thus at the stage that an interested person contacts a service provider to get further information on a service or goods and the communication does not require personal information, in particular if the inquiry is done online and thus no mailing address is needed. The retrieval of answers should be possible anonymously as well.

Stage 2 refers to all cases where proof is necessary, that the same person is acting at a later point of time. This may be accomplished by a means to recognize the person which is currently done with cookies or a pseudonymous username and password combination. The nPA provides for a specific pseudonym function allowing the proof that the same person is acting. Such a proof may be required for early contact negotiations where an interested person asks for a personalized service such as the conditions for a personalized insurance contract. Here the data controller does not need to know the identity of the interested person until the interested person decides to conclude the contract under the conditions offered.

At Stage 3 some kind of auf authentication of the holder is required, e.g., being of a certain age for viewing age restricted previews on a video portal or the proof is needed of being domiciled in a certain municipality for accessing services reserved to its citizens. At this stage the holder may still remain anonymous as only the requested information is necessary but not an identification of the person acting.

Stage 4 requires an identification of the holder which may be the case when the service provider bears a financial risk due to delivering the service prior to receiving full consideration in return or where identification is required by law. In relation to public authorities a clear identification is always necessary when an administrative act addresses just a single person.

The described pattern has been derived from typical negotiation processes where the stages often follow each other in a chronological order and seem to correlate with specific needs to gain information about the other party. But the stages may also appear in parallel and will then relate to different purposes such as an age verification required by law or the need to collect the address to ensure payment.

Summarizing the conclusions from the model, it can be said that when assessing the necessity for a certain data processing due regard must also be held to the stages of the underlying negotiation process. Often it may not be not necessary to collect personal data immediately but rather at a later point. For the German nPA the conclusion has to be drawn that some data controllers may need more than a single certificate for certain business cases. For example allowing access to age restricted video previews on a website only requires the anonymous age verification but another certificate is needed to identify the holder when she eventually subscribes to the service.

2.3 Disclosures to third parties

An imminent danger, also seen by the legislator, is that the verified information may be disclosed to third parties. In consequence the service provider may even become an

identity provider herself thus undermining the security measures of the nPA. There are business models imaginable which are well justifiable and probably even beneficiary to the holders such as having verified identities on online auction platforms for increased trust. However, a transfer of the collected data to third persons would usually constitute a change of purposes and thus lay beyond the purposes for which the authorization has been issued and is not permissible, § 21 sec. 2 no. 1 PAuswG.

An interesting legal question in this context is whether holders may allow such a change of purposes by means of informed consent. While consent in the sense of the DPD is system immanent for the nPA, as it is required for every transaction and ensured by the requirement to show the service provider's access certificate before the holder may even enter her PIN to release the data. It is not, however, mentioned that consent may replace the proof of the necessity for clearly specified purposes. While the German legislator blocked processing for purposes of business-like transfer of data to third parties (e.g., address brokers or credit rating agencies) with the provision in § 21 sec. 2 no. 2 PAuswG [3, p. 43], it is not so clear whether uses such as having verified identities on social networks or online auction platforms may constitute an acceptable purpose. On the one hand one should bear in mind the danger that third party identity providers will undermine the security measures provided with the nPA and its underlying infrastructure. On the other hand introducing eIDs in Germany and other Member States of the European Union aims at making identification of oneself in electronic interactions easier so these opportunities for a voluntary identification should not be limited in an overdue manner. In particular having a verified identity in communities where participants other than the service provider itself rely on such information, should be possible. But the holder must still retain power over the provided information and the data must only be passed on to third parties in certain predefined cases such as breach of contract. The holder must be able to revoke the consent for the future or for future transactions respectively. Besides this she should still be able to act under a pseudonym

2.4 Enforcement of limitations

To be effective the limitations on the use of personal data attained from an nPA require enforcement and continuous control by the responsible public authorities. For this the German law provides for possibilities to revoke authorizations and the BVA and federal and state data protection authorities (DPA) should stay in contact to ensure interpretation of the law consistent with the DPAs' view on processing of personal data outside of the limited scope of application of the nPA.

In respect to the enforcement of the limitations the German law provides that the authorization and in consequence any certificate issued on basis of the respective authorization must be revoked if the service provider received it by providing false information or if it should not have been issued according to the law in the first place, § 21 sec. 5 PAuswG. Besides these cases, the authorization should be revoked when the DPA for the specific service provider demands this as facts indicate that the service provider processes the data in an illegal manner, § 21 sec. 5 PAuswG. While all other legal instruments provided to the DPAs to react to illegal processing of personal data such as administrative fines remain unaffected and should be deployed

as appropriate in a given case, the specific measure of asking the BVA to revoke authorizations should always be duly considered by DPAs whenever data retrieved from nPA are subject matter of the illegal processing.

Even though § 21 sec. 5 PAuswG provides for a measure to correct individual decisions by the BVA in case of illegal processing, it seems preferable to maintain an ongoing information exchange between the BVA and the DPAs. For individual cases such a collaboration is already stipulated in § 29 sec. 3 of the German Personalausweisverordnung (PAuswV, German Regulation on Identity Cards). This allows the BVA to obtain a comment of the competent DPA whether a specific service provider applying for an authorization is known for practices of illegal processing. Further, periodical meetings between the BVA and representatives of the DPAs to exchange experiences and opinions are highly recommendable.

3 Necessary data processing – standard use case

Some standard business applications and use cases have been analyzed and evaluated in [8]. In the following the most central use cases will be shortly introduced showing the practicability of the staged model described above. The use cases have been drafted with the nPA in mind, but they may also aid to the understanding of what constitutes necessary data processing in general. So far the necessity of data processing has been analyzed in Germany for a set of individual cases, however, none of which directly related to applications of the nPA. The general rule used so far in data protection law is rather vague and states that processing is not necessary if a purpose may be reached without deployment of personal data in particular as an adequate and reasonable alternative is equally or even better able to serve the desired purpose [10 at § 28 BDSG para. 14 et seq. with further references and historic overview][11 at § 28 BDSG para. 48].

3.1 Cases where the law requires an identification

Processing of personal data is generally allowed where specifically required by legal provisions.[5] Some legal regulations require that the service provider identifies or authenticates[6] its customers. This is for example the case for telecommunication service providers in Germany that are required by law to collect name and address for potential inquires by public authorities.[7] Also German banks are required to identify customers opening an account due to regulations against tax fraud[8] and money laundering[9]. According to the principle of purpose limitation set forth in Art. 6 sec. 1 b DPD, the data collected for such purposes must be stored separately from other

[5] Cf. Art. 7 c) DPD.
[6] E.g., age verification in case of content or goods reserved for adults.
[7] See for Germany § 111 TKG (Law on Telecommunication).
[8] See § 154 AO (Abgabenordnung = German General Tax Code).
[9] See § 3 sec. 1 GWG (Geldwäschegesetz = German Prevention of Money Laundering Act)

personal data and must not be used for other than the legally required purposes which made collecting the data necessary [cf. 6 sec. 2.89 et seq.][12, p. 49].

3.2 Exchange of goods and services

For the probably most frequent transaction in practice, the exchange of goods or services for payment, an identification of the customer is necessary only when one party bears the risk of not getting the agreed benefit in return. This is particularly the case when one party is obliged to perform the contract before the other party. Filing a lawsuit against the customer may then become necessary. For this the civil procedural codes of the Member States presently require that name and address of the debtor must be indicated.[10] Also within European civil procedural law it is accepted doctrine that the defendant must be served with the document which institutes the proceedings in sufficient time and in such a way as to enable him to arrange for his defense or otherwise recognition and enforcement of a judgment may be declined.[11] In the absence of other reliable means to serve such documents knowledge of the name and address of a potential defendant can be deemed necessary. For the mentioned cases of pre-performance of the selling party the necessity of accessing data stored in the buyer's nPA must be accepted while in cases where a risk of loss of payment is absent it may not be necessary to process personal data at all. In particular such a necessity cannot be derived solely from the fact of having concluded a contract with the data subject. This assumption is also backed by German and European data protection law which allows processing of personal data only to the extent necessary for the performance of a contract to which the data subject is party, see § 28 sec. 1 no. 1 BDSG and Art. 7 lit. b) DPD.

The flowchart in Figure 1 below shows how to assess whether a risk for a loss of payment may be assumed for the service provider making the processing of personal data from the nPA necessary. Note that in the opposite direction customers of services or goods are usually allowed to identify the service provider as the law grants the customer guarantees and other rights and remedies in case the service or goods lack conformity[12] while the rights of the service provider usually extend only to the full and timely payment.

As any processing that is required by law (see 3.1) to identify or authenticate customers is necessary this question must be answered first and independent from the risk of financial losses. If no duty to identify the customer exists and the service provider has fully received the payment, e.g., in cases of prepayment via bank transfer, processing of any personal data cannot be considered necessary. The same is true when a safe payment method is chosen that ensures that the service provider receives the payment, e.g., if the credit card company bindingly acknowledged the

[10] See for Germany § 253 sec. 1 ZPO (Civil Procedural Code).

[11] Art. 34 no. 2 of the Council Regulation (EC) No 44/2001of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Regulation), see also the almost identical rules in the so called Lugano Convention of 1988 applicable in relation to Iceland, Norway and Switzerland.

[12] In relation to consumers within the European Union see Art. 3 et seq. of Directive 1999/44/EC and other directives strengthening the rights of consumers.

transfer or if the payment is done in direct exchange for the goods. If, however, a financial risk remains for the service provider, identifying information required to raise a civil lawsuit (name, address, as well as the date of birth) are necessary and may be processed.

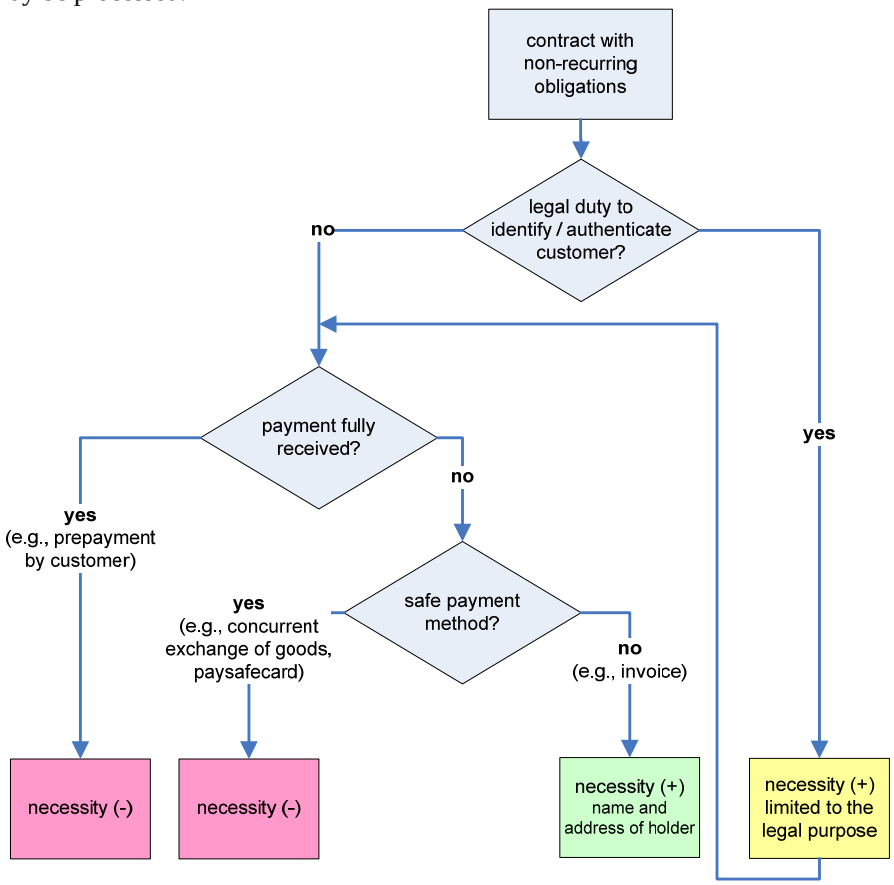

Figure 1: Necessity to process personal data for contracts with non-recurring obligations

The necessity to collect name and address of contractual partners due to the potential need to file an action in court may fall away once alternatives for the reliable service of documents become available. In Germany a draft Act for a verified form of e-mail is currently in the parliamentary process.[13] The so-called De-Mail service will provide a proof valid in court proceedings that a document has been received by the addressee. In consequence Art. 2 of the current draft of the De-Mail Act provides an amendment to § 174 sec. 3 German Code of Civil Procedure (ZPO) allowing service

[13] Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften as of October 13th, 2010, available online: http://www.bmi.bund.de/SharedDocs/Gesetzestexte/_Gesetzesentwuerfe/Entwurf_Demail.html.

of documents (law: the formal delivery of a document such as a writ of summons) via the De-Mail service. Whether this will lead to the consequence that users of the De-Mail service may provide the De-Mail address instead of the name and address and which consequences follow for existing authorizations needs to be evaluated in the future.

3.3 Contracts with recurring obligations

Similarly in contracts with recurring obligations a need for identifying information may be given, particularly if one party is obliged to advance performance and thus has a risk of not receiving what has been promised in return. However, some specialties of recurring obligations should be taken into account. The necessary decisions to assess whether processing of personal data is necessary are displayed in Figure 2.

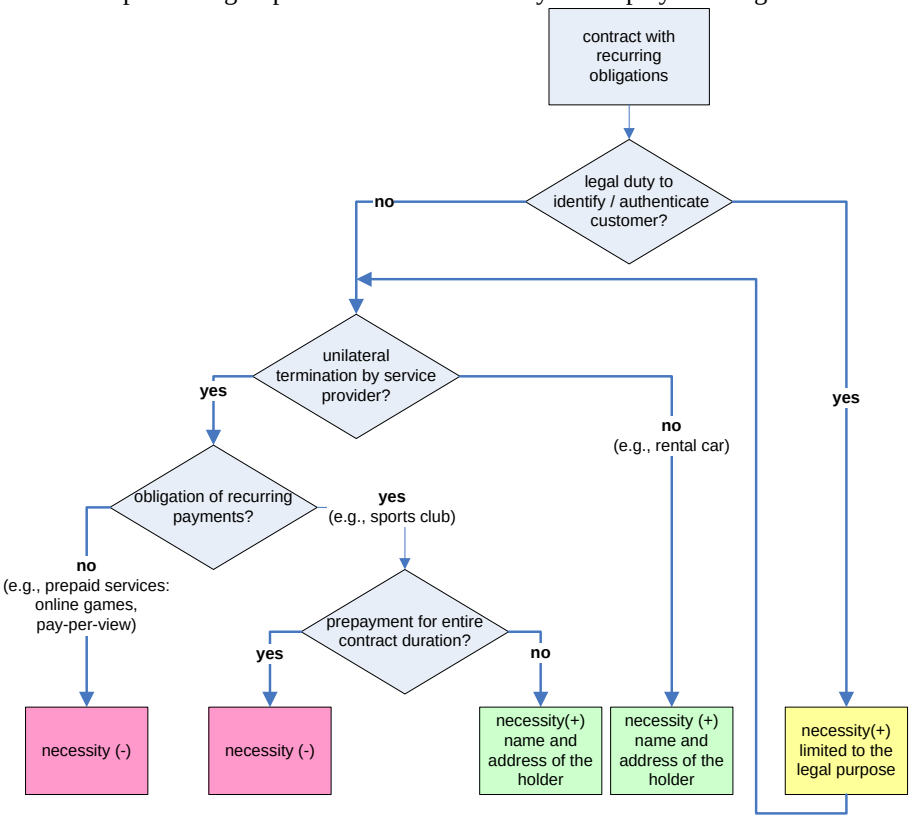

Figure 2: Necessity to process personal data for contracts with recurring obligations

Again a legal duty to identify or authenticate the customer always allows the collection and processing of personal data, while the use of this information is limited

to fulfilling the said legal requirements. For contracts with recurring obligations the risk for the service provider differs from contracts described in section 3.2 above when she is legally allowed and able in fact to terminate the service immediately and unilaterally (e.g., pay-per-view services, prepaid mobile phone cards). A substantially higher risk for the service provider must be accepted where she is unable to withhold the service unilaterally as for example goods need to be returned (e.g., a rented car). A financial risk may even exist when the provider is able to terminate the performance unilaterally but the customer is bound for a fixed duration and obliged to pay for the whole period of the contract irrespective of quitting the use of the service (e.g., membership in fitness clubs or newspaper subscriptions with a fixed duration). In this case the service provider runs the risk of not receiving the whole payment unless the customer has paid for the whole period in advance.

3.4 Pseudonymous access

Besides providing the classical identifying personal data, the nPA also offers the possibility to use pseudonyms. The pseudonyms generated from the certificates of the held by the service provider and stored on the user's nPA allow a secure re-identification of a holder using the nPA by a service provider. Anytime where the primary use of the nPA is to securely re-identify a person, the pseudonym should be used instead of other personal data from the nPA, thus making it unnecessary to collect data such as the (verified) name and address. The pseudonyms will be created for every relation of an nPA and a service provider, thus avoiding any risk to link a holder's activities across websites of different providers.

With the pseudonym function the nPA offers a secure token-based method for authentications. But the effective necessity for such functionality will have to be seen in practice. At present cookies provide a similar functionality of re-identifying a user, at least wherever the sensitivity of a service does not require a more secure token-based authentication. While non-sensitive services such as virtual shopping carts for online stores may be implemented with cookies this evaluation will change for more personalized services. A potential use case for the pseudonym function of the nPA may be the request for individual insurance conditions by providing data such as age, weight or previous diseases without disclosing ones identity. The secure re-identification will then allow retrieval of calculated individual insurance rates and the conclusion of the contract under the previously stipulated conditions.

The current version of the nPA does not allow disclosing the identity of the holder using a pseudonym in case this may become necessary. This may be the case if disputes arise requiring a civil lawsuit. Lacking the capability to reveal the true identity of the holder under certain predefined conditions the pseudonym function will not be able to replace the verified name and address in the abovementioned contractual relationships. If eventually future versions of the German nPA or other European eID schemas offer such recoverable pseudonyms, the necessity to process personal data must be reconsidered. In this case it would be very desirable from a privacy perspective if the recoverable pseudonym would not substitute the existing pseudonym but rather complement it for the use cases mentioned above.

3.5 Claiming the right of access

The nPA will also be useful for verifying that only the authorized person claims the right of access to her personal data as granted by Art. 12 DPD and § 34 German Federal Data Protection Act (BDSG). But identifying oneself in general or even using the nPA must not become a prerequisite for claiming the right of access granted by the DPD. Rather the data controller has to send the requested information to the address stored in his system unless there is doubt regarding the identity of the requesting data subject, e.g., when persons with identical names and birthdates appear in the database [11 at § 34 BDSG para. 26]. Identification with the nPA will be necessary if the information is asked to be transferred elsewhere than to the address registered with the data controller. The nPA may in particular promote the right of access insofar as it enables data controllers to offer easy access to data subjects in online environments and eventually in real time. But again data controllers must not use the data collected for the identification of the requesting person for other purposes than complying with the right of access. In particular the data provided must not be used to update or complement existing customer data.

5 Conclusion and outlook

The model described in section 2.2 above allows the assessment of the necessity to process personal data in a variety of use cases. It provides a first refinement and aid for legal practitioners that need to evaluate the question of necessity in a given case. In particular the model allows checking whether less information may suffice. A central finding that needs to be communicated to the legal practice is that the amount of data required depends massively on the stage within the process of contractual negotiation. As there is no need to collect information about customers that just seek for first information on goods or services, it is in consequence not allowed to force users to disclose personal data unless a contract is concluded (see above sections 3.2 and 3.3). For the nPA this will mean that businesses cases in which earlier stages of the negotiation require a safe identification will need more than one certificate to collect the data from the nPA.

The anonymous proof of the holder's age and place of living provided by the nPA is a major advancement for the user's privacy as it makes more detailed identifications unnecessary when actually only an age verification is required. From the privacy viewpoint a desirable improvement of the nPA would be the support of the anonymous credential technology as is currently provided by IBM's Identity Mixer[14] and Microsoft's U-Prove[15] system. This would allow for anonymous authentication of claims such as being member student of a certain university or employee of a certain entity. Here the nPA might be of value in the process of attaining these certificates online from the issuer (a trusted party, e.g., the

[14] Binaries, source code and documentation are available online at: http://www.primelife.eu/results/opensource/55-identity-mixer.

[15] Documentation available online: http://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26953.

university).[16] Once such a technology is widely available, a re-evaluation of the necessity of data processing will presumably show that in many cases processing of personal data may become dispensable as anonymous credentials issued by a trusted party can replace the identification while still providing the needed security and trust.

6 References

1. Naumann, I. (ed.): Privacy and Security Risks when Authenticating on the Internet with European eID Cards. ENISA Risk Assessment Report, online: http://www.enisa.europa.eu/act/it/eid/eid-online-banking (2009)
2. Kubicek, H., Noack, T.: The path dependency of national electronic identities. In: Identity in the Information Society (IDIS), pp. 111-153. Available online: http://www.springerlink.com/content/17t6467515511359/fulltext.pdf (2010)
3. Bundesregierung (German Federal Government): Entwurf eines Gesetzes über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften (reasoning for German Law on Identity Cards). In: Bundestagsdrucksache (BT-Ducks.) 16/10489, online: http://dipbt.bundestag.de/dip21/btd/16/104/1610489.pdf (2008)
4. Leenes, R., Schallaböck, J., Hansen, M. (eds): PRIME White Paper. Deliverable of the Project PRIME – Privacy and Identity Management for Europe. Available online: https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf (2008)
5. Rost, M., Pfitzmann, A.: Datenschutz-Schutzziele – Revisited. In: Datenschutz und Datensicherheit (DuD), Vol. 33, No. 6, pp. 353-358. Available online: http://www.maroki.de/pub/privacy/DuD0906_Schutzziele.pdf (2009)
6. Kuner, C.: European Data Protection Law: Corporate Compliance and Regulation. Oxford University Press, USA, 2nd edition (2007)
7. Polenz, S.: Der neue elektronische Personalausweis. E-Government im Scheckkartenformat. In: Multimedia und Recht (MMR) Nr. 10, pp. 671-676. Available online: http://beck-online.beck.de/ (2010)
8. Ad-hoc working party of the German data protection authorities: Datenschutzrechtliche Leitlinien für die Erteilung von Berechtigungen nach § 21 Abs. 2 PAuswG aus Sicht der Ad-hoc-Arbeitsgruppe nPA der Datenschutzbeauftragten des Bundes und der Länder. Final version as of September 10th, 2010. Available online: www.datenschutzzentrum.de/neuer-personalausweis/ (2010)
9. Fischer-Hübner, S., Zwingelberg, H. (eds.): UI Prototypes: Policy Administration and Presentation – Version 2. PrimeLife Deliverable D4.3.2. Available online: http://www.primelife.eu/results/documents (2010)
10. Gola, P., Klug, C., Körffer, B., Schomerus, R.: BDSG Bundesdatenschutzgesetz – Kommentar. Beck, Munich, Germany, 10th edition, (2010)
11. Däubler, W., Klebe, T. Wedde, P., Weichert, T.: Bundesdatenschutzgesetz – Kompaktkommentar zum BDSG. Bund, Frankfurt, Germany, 3rd edition (2010)
12. Carey, P.: Data Protection – A Practical Guide to UK and EU Law, Oxford, (2009)

[16] A project providing a connection between the nPA and U-Prove has recently received the "TeleTrusT Innovation Award", http://www.heise.de/security/meldung/ISSE-2010-Innovationspreis-fuer-Fraunhofer-Projekt-zum-neuen-Personalausweis-Update-1104004.html. The European project ABC4Trust which was launched in November 2010 will take up PrimeLife results on anonymous credentials and address the challenge of interoperability between different credential systems, see www.abc4trust.eu.