"Identity Management by Design" with a Technical Mediator Under the GDPR

Anne Steinbrück

"Identity management by design" with a technical Mediator under the GDPR

Dr. iur. Anne Steinbrück[1] [✉]

[1] Karlsruhe Institute of Technology, Center of advanced legal studies, Germany

anne.steinbrueck@kit.edu

Abstract. The Charter of Fundamental Rights of the European Union (CFR) and the GDPR refer to the protection of personal data and personal identities. In the General Data Protection Regulation (GDPR) the term of personal data contains the protection of the physical, physiological, genetic, psychological, economic, cultural and social identities, Art. 4 para. 1 GDPR. This legal definition introduces the understanding of "identity" in a pluralistic sense. Thus, the notion of pluralistic and dynamic identities should be translated in a "*privacy by design*" mechanism. This notion of pluralistic identities would mirror a differentiated protection for personal identities based the right of informational self-determination, Art. 7, 8 CFR. Thus, the data subject should be enabled to develop the personal identity in an online-context in the same manner as it is done in an offline-context. This includes the opportunity for the data subject to control personal identities in their static "*Idem*-part" such as the name and their dynamic "*Ipse*-part" realized by the behavior (based on the philosophical theory by *Ricœur*). These parts of the personal identity should be visualized with a "dashboard" that allows the data subject to control and manage the personal identities. This "dashboard" should include an impartial technical mediator that embodies an effective, non-discriminatory and structured process. Such a technical mediator should be specified in an "*identity management by design*" mechanism based on Art. 25 GDPR in order to achieve an effective privacy protection in the era of Big Data.

Keywords: Privacy by Design, Identity Protection, Human Rights, Mediation, Game Theory.

1. Introduction

The Charter of Fundamental Rights of the European Union (CFR) and the General Data Protection Regulation (GDPR) protect personal data. At the same time, the protection of personal data in the definition of Art. 4 para. 1 GDPR embodies the notion that personal data can be factors of physical, physiological, genetic, psychological, economic, cultural and social identity. Thus, the CFR and the GDPR include the notion of pluralistic identities, because personal identities can be realized in many contexts and have to be protected as such. Comparing the protection of personal identities in an offline- and online-context, in an online-context there is a lack of transparency

regarding the profiles and personal identities. In particular profiles based on user behavior in social media are the origins for advertisements or feeds and remain unknown for the data subject, as it became obvious in the *Cambridge Analytica* case [34]. These advertisements or feeds based on profiles are often the result of user behavior that is unconscious ("digital unconscious" [14]) rather than rational. The user might assume to be able to fully exercise his fundamental rights, but in fact remains unprotected with respect to the profiles created by the controller. The gap between theoretical protection of users and generated profiles requires a differentiated protection of context specific generated profiles as identities. The question should be examined, how to describe an effective protection regime for the online-specific usage of pluralistic identities for each context. Such a protection regime should fulfill the requirement of self-determination based on Art. 7, 8 CFR.

To describe a protection regime, existing legal perspectives on privacy and identity protection should be evaluated. The research from other disciplines should also be included to reflect the phenomena of identities in the online-context and define an effective mechanism for protection. First it should be shown that the concept of plural identities can be described by the term "dynamic identity" (2.). Furthermore, the dynamics of identities in each context in the GDPR should be determined, so that the *"contextual integrity"* of personal identities will be described (3.). Consequently, the protection of personal identities in an offline- and online-context and the term of dynamic identity should be included in the technological and organizational measures. This could be realized with a specific concept of *"privacy by design"* based on Art. 25 GDRP, which covers the protection of dynamic identities with a *"identity management by design"* mechanism (4.). Such a mechanism should include a "technical mediator" in order to implement ethical and human rights standard for a dynamic identity protection based on the Charter of Fundamental Rights to effectively protect personal identities in the era of Big Data (5.). Finally, the requirements for an effective protection of dynamic identities should introduce a paradigm shift towards a differentiated identity protection in the GDPR (6.).

2. The term "*dynamic identities*"

2.1. The term "*dynamic identities*" in the Charter of Fundamental Rights

The protection of personal data based on Art. 8 CFR contains the definition of personal data under the secondary law of the GDPR, so that the economic, physiological and psychological identities are also protectedly Art. 8 CFR [17], [24]. The "self-determination of the individual with regard to his or her data" was recognized in the deliberations of the Charter of Fundamental Rights to be protected by Art. 8 CFR [5]. To exercise self-determination is covered in data protection law by the concept of consent, Art. 6, 7 GDPR. The consent justifies the processing and that context-specific personal identities are generated. Subsequently, the control by the data subject is strengthened by the exercise of the data subject rights in accordance with Art. 8 para. 2 s. 2 CFR in order to determine the personal identities.

In particular, control includes the right to be forgotten, which is fundamental for the protection of personal identities: The right to a new beginning in the sense of a *tabula rasa*-right is decisive for a new beginning in the online-context, and is reflected in the recent decision of the German Constitutional Court on the "Right to Forget I" (German Constitutional Court, Judgment, November 09, 2019, No. 1 BvR 16/13). It was held that with regard to past crimes and the past imprisonment, there must be a chance for a new beginning. The new beginning has to include the right to forget, so that an article regarding the crime in an archive that is online available can be deleted. Consequently, the term of dynamic identities covers the right of a new beginning in an online- and offline-context.

According to Art. 7 CFR, private life and communication are protected. The protection of the private life includes that the identity shall be constituted and determined by oneself [17]. This makes clear that, in addition to identity as a name the term identity includes the dynamic part of the personality realized in online- and offline-contexts. In addition, the Convent of the Charter of Fundamental Rights discussed the inclusion of the wording "identity" in Art. 7 CFR [5]. However, since the term of identity is rarely used in the wording of the constitutions of the Member States, the Convent has distanced itself from this. So the term of identity in its "individual uniqueness" of personalities is part of the right to informational self-determination based on Art. 7, 8 CFR [5]. Thus, personal identities and the possibilities for personal development are protected for the online-context in the same way as in the offline-context. In particular the right to be forgotten allows an individual to leave past behaviors behind and to have the chance of a new beginning. Accordingly, it is inherent that the Charter of Fundamental Rights includes the protection of personal identity in a dynamic and communicative dimension [5], [17]. This applies in particular to the online-context, which is also covered with regard to new developments by the protection of Art. 7, 8 CFR [5]. Conclusively, the term of dynamic personal identities is part of the protection regime of the Charter of Fundamental Rights.

2.2. The term identity from an interdisciplinary perspective

Information technology perspective. The term "identity" describes the process of comparison in order to determine perfect equality between two objects. Taking the perspective of information technology into account, identity is primarily understood as the process of identification and authentication [37]. The process of identification and authentication provide access rights that are often called "digital identities" [16], [37]. These "digital identities" represent the numerical part of a personal identity during a life cycle. Thus, the term identity in the perspective of information technologies includes the numerical part of identity, which corresponds with a static understanding of identity. This static understanding of identity can be seen by calling electronic ID-cards "digital identities" [16]. With such static digital identities trust regarding the correctness of the identity can be established. A high degree of trust can be particularly applied by issuing electronic signatures. Also employee-IDs are examples for static and numeric identities that enable certain access rights.

Thus, identities from an information technological perspective include the management of access rights [37]. In conclusion the informational technology perspective embodies a static notion on identity and the concrete content of the personal identity is of secondary importance.

Philosophical perspective. The static perspective on identity is expanded with the notion of a dynamic personal identity by the philosophical model of *Ricœur* (Fig. 1). The concept of identity is differentiated between a numerical part of equality (*Idem*) and a behavioral part of selfhood (*Ipse*) [31], [15], [20]. The *Ipse*-part is defined by the interaction with others and the *Idem*-part particularly describes the process of identification with a high degree of credibility and reputation [15]. This philosophical differentiation between the "dynamic" *Ipse*- and the "static" *Idem*-part of an identity illustrates the expressions of identity. In particular, the *Idem*-part of identity is the name and it responds to the question of "who?" [31]. The *Ipse*- and *Idem*-part of identity together constitute the character of a person that mediates both identity parts [31]. Thus, the character is the result of a dialectic relation between the static *Idem*- and dynamic *Ipse*- part of identity [31]. This character is the source of the temporary action that becomes visible for others [21]. With the temporary action the self-presentation and the communication with others the identity is subject to an iterative dialogue [21]. This dynamic of an iterative dialogue is one source for the personal development, which is taking place in an online- and offline-context equally [14]. This differentiated philosophical perspective of identity is mirrored in the definition of personal data in Art. 8 para. 1 CFR and should be subject to the technical mechanism of *"identity management by design"*.

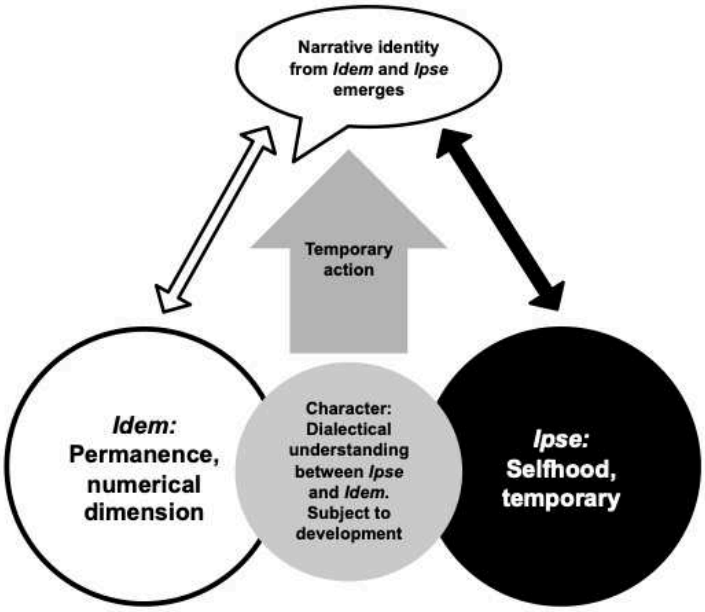

Fig. 1. Model of the term identity by *Ricœur,* "Oneself as another".

Social-psychological perspective. In addition, the social-psychological and the communication psychology perspective on personal identity stress the dynamic aspect of identity [22], [36]. In general the social-psychological understanding of identity depends on the current social-psychological schools. For example, the school of *Erikson* [9] assumes the formation of identity in eight phases, which can have an effect on the later personality and possible conflicts. This school understands identity as "inner capital" that is formed in the childhood and adolescence so that an "unitary identity" [18] is the result. This school is contrasted by the modern theoretical understanding of personal identity, which is characterized by a continuous identity formation in life. The identity is subject to continuous formation by internal and external social structures. Consequently, personal identity defines itself in a dialog and is in continuous construction, so that identity emerges from actions and narratives [20]. From a psychological perspective identity can be summarized as a "I am many", which is constituted by a social self, professional self, a physical self and a religious self [21], [19]. This understanding of many identities includes the different realization of identity in each context and its dependency on the communicative relationship. This allows a dynamic identity building [21], that gives the personal identity an amoeba-like character. However, these characteristics of dynamic personal identity in an offline-context should also be reflected in an online-context.

It has been observed that there is an online-specific shift in identity building. In particular, the de-territorialized internet usage has made it easier to find social contacts and to present the own identity in the desired image. One reason for this change in the individual behavior is stated to be the cognitive distortion while using the internet and that it is easy to establish virtual identities [35]. This makes identity experiments possible, which can influence the development of personal identities [35].

Conclusively, the social-psychological perspective on personal identity includes a dynamic understanding of many identities. These personal identities are realized in communicative relationships in an offline- and online-context. In an online-context the communication can be influenced by the interface design so that cognitive distortion can influence the realization of identities.

2.3. "*Dynamic Identity*" in the GDPR

The definition in Art. 4 para. 1 GDPR includes, in addition to the protection of personal data, a context-specific concept of identity that classifies economic, cultural and social identity as worthy of protection. Taking the contexts for the identities into account, it seems that the notion of many identities in a communicative relation is immanent to the GDPR. This is also visible with the definition of special categories of personal data under Art. 9 GDPR, according to which the expression of political opinions, religious, ideological beliefs, trade union membership or health data enjoy a higher level of protection. The different identities defined in Art. 4 para. 1 GDPR and the different special categories of personal data defined in Art. 9 GDPR express beha-

vior related *Ipse*-parts of a personal identity. These *Ipse*-parts of a personal identity depend on the context and may temporarily appear and disappear.

Also profiles as defined in Art. 4 para. 4 GDPR stipulate a dynamic behavioral oriented understanding of personal identity. Such profiles are constituted out of algorithm-based deconstructions and combinations of characteristics of a personal identity. Even the use of pseudonyms (Art. 4 para. 5 GDPR) demonstrates the *Idem*-part of the identity as a static identifier, and the temporary use of the identifier establishes the dynamic *Ipse*-part of the personal identity. In conclusion the GDPR embodies the notion of a dynamic personal identity that is subject to the protection regime of the GDPR.

2.4. Protection of dynamic identities

The term of dynamic identities has its source in the protection of personal data and private life based on Art. 7, 8 CFR. Thus, personal identities are protected by the European Charter of Fundamental Rights not only regarding the static name, but also the dynamic part of personality and identity building behavior are covered. Taking the interdisciplinary perspective into account, in particular the model by *Ricœur* allows a clear differentiation between static *Idem*- and dynamic *Ipse*-parts of personal identity. The model by *Ricœur* reflects the protective regime of personal data and private life, Art. 7, 8 CFR. Also the social-psychological perspective includes a broad understanding of personal identity that depends on the communicative relationship that constitutes several identities. Consequently, the term of dynamic personal identities is reflecting the interdisciplinary understanding of identity and is protected by the Charter of Fundamental Rights and the GDPR. In addition, the protection of the static *Idem*- and dynamic *Ipse*-parts of personal identity also depends on the context the identity is realized.

3. Contextual protection of dynamic identities in the GDPR

The GDPR explicitly differentiates between the economic, social, health and professional context, Art. 4 para. 1, Art. 88 GDPR. In addition the activities in the private and family context are out of the scope of GDPR, Art. 2 para. 2 c) GDPR. However, the processing of personal data in a private context falls within the scope of the GDPR if the context changes towards e.g. social media or a business environment. Such a change of the context can evolve gradually, making it impossible to distinguish clearly whether it falls within the scope of the GDPR. But in order to apply the protective regime of the GDPR Art. 2 para. 2 c) must be interpreted narrowly, as it was stipulated by the European Court of Justice (ECJ) in the *Linquist*-decision (ECJ, 06. November 2003 - C-101/01). In this judgment it was held that private information even though it is presented in a slightly humorous way on a website, has to be considered in scope with the Data Protection Directive.

Furthermore, the GDPR provides with Art. 88 GDPR a specific regulation for the context of employment. The requirements under Art. 88 GDPR include the phases of

application, hiring, work relation and termination of the contract [25]. Therefore in the employment context several static *Idem*-parts of personal identity are required. These include the health insurance number, tax identification number, and social security number as *Idem*-parts of personal identity.

These different contexts in the GDPR illustrate that the *Idem*- and *Ipse*-parts of the identity have to be controlled by the data subject in order to make use of the right of informational self-determination. With an identity management scheme that includes both the static *Idem*- and dynamic *Ipse*-part of personal identity the integrity of the personality can be realized in each context. In order to reach a high level of identity protection the principle of data minimization (Art. 5 para. 1 c) GDPR) would be implemented by a context specific identity management. This would establish a contextual integrity of personal identities. In addition, the contextual identities would be kept separate, so that the specific needs of protection in each context would be realized. Such a mechanism is described by *Nissenbaum's* concept of "contextual integrity" [26] that differentiates between different degrees of protection and context-specific "justice". Under this concept privacy can be realized in an official, professional and private communication and the specific information depends on the definition of the context. Such a mechanism is described by *Nissenbaum's* concept of "contextual integrity" [26] that differentiates between different degrees of protection and context-specific "justice". Under this concept privacy can be realized in an official, professional and private communication and the specific information depends on the definition of the context. Thus, the concept of "contextual integrity" includes the control of the degree of publicity of the information and the access level to sensitive and confidential contexts.

Finally, the management of the dynamic *Ipse*- and static *Idem*-part of a personal identity the contextual integrity should be maintained. In order to effectively implement contextual integrity in an identity management system, the technology has to be adjusted to the concept of static *Idem*- and dynamic *Ipse*-identities. Therefore the concept of "*privacy by design*" based on Art. 25 GDPR, recital 78 s. 2 might give fundamental guidance.

4. *"Identity management by design"* based on Art. 25 GDPR

The concepts of *"privacy by design"* and *"privacy by default"* are part of Art. 25 GDPR, recital 78 s. 2 and stipulate the technological implementation of the principles of data processing pursuant to Art. 5 para. 1 GDPR. This includes the application into the technical and organizational design pursuant to Art. 25, 5 para. 1 GDPR.

In order to increase the level of protection for data subjects the concept of *Idem*- and *Ipse*-identities should be applied in the technical design of the processing. This includes a technical design that enables the data subject to control the personal identities with access rights as part of the principle of transparency, Art. 5 para. 1 a), 12, 15 GDPR. In order to reach a high level of identity protection it would be reasonable to provide access e.g. to the profiles as *Ipse*-parts of the personal identity. This enables the data subject to gain information and knowledge about existing profiles in order to

exercise control on the identities. The reason is that the data subject might not be aware about the impact of the profiles to the personal preferences [15].

The data subject has the opportunity of an iterative control on personal identities and the right to agree or disagree with a profile of the identity. Such a mechanism as "*identity management by design*" would make personal identities dynamic and negotiable. It would be desirable that the "*identity management by design*" mechanism would become the "best practice" version from a bundle of measures by determining the appropriate state of the art. This approach goes beyond the traditional identity management referring to access management by identification or authentication. The "*identity management by design*" should include a mechanism that allows the iterative negotiation of personal identities. Consequently, the mechanism of *"identity management by design"* serves the fundamental transparency requirement under Art. 5 para. 1 a) GDPR. With the transparency of personal identities created by the "*identity management by design"* mechanism the self-determination can be exercised effectively. With the information about the generated profiles the data subject can decide whether to agree to this *Ipse*-part of the personal identity or disagree. The decision of the data subject on the personal identities is extended by the rights of the data subject pursuant to Art. 15–21 GDPR.

In particular, a "dashboard" as proposed by *Raschke/Küpper/Drozd/Kirrane* would be a reasonable solution [28]. With this "dashboard" the data subject is enabled to manage the rights such as the right to information, the consent and the rights of the data subject pursuant to Art. 15–21 GDPR. In order to protect personal identities, it would be desirable to extent such a "dashboard" with the transparency of personal identities and the iterative control over the *Ipse*- and *Idem*-parts of personal identity. Such a "dashboard" could also raise awareness and be applied as a tool for risk minimization based on Art. 32 para. 2 GDPR.

In general, the mechanism *"identity management by design"* would ensure that the *Ipse*-parts of identities are kept dynamic. This is possible by providing the transparency of the identities and by keeping the identities negotiable. For this the mechanism of *"identity management by design"* a technical mediator should be included in order to guarantee the negotiability of the *Ipse*-parts of personal identity.

5. Negotiable personal identities with a technical Mediator

The need to negotiate personal identities presumes an environment for cooperation. The concept of cooperation is subject to the GDPR (5.1.). Furthermore, the relationship between the controller and the data subject has to be defined (5.2.). Then the resolution of the different interests in this relationship has to be analyzed in order to create a cooperation environment (5.3.). This could follow by the increase of the iterations in accordance with the "TIT for TAT"-strategy [2] and the transfer into a solution with a technical mediator.

5.1. Cooperation in the GDPR

The concept of cooperation is anchored in the GDPR. It has the function to build a trustful relationship in order to widen the possible solutions. Thus, cooperation is recognized as an important factor in creating value and potential [8]. According to Art. 31 GDPR the controller shall "cooperate" with the supervisory authority regarding the performance of its legal duties. Furthermore, Art. 33 para. 4 GDPR expresses the communicative exchange with the supervisory authority. In particular, the information in case of a breach of the data processing principles may be provided progressively to the supervisory authority. On this way the solution of the problem becomes a "shared mission" [7] between controller and supervisory authority. The potential conflict becomes a challenge of the controller and supervisory authority equally. Therefore, the stipulation of "cooperation" provides a procedure that allows self-regulation in the rapidly changing environment of information technologies [33]. Consequently, the promotion of cooperation is a recognized concept in the GDPR.

For the protection of personal identities, a cooperative procedure could be an essential part in the mechanism of *"identity management by design"*. Since cooperation creates value, a cooperative environment would be beneficial for the protection of personal identities. This mechanism of *"identity management by design"* could create an environment for diverse personal identities. In this respect, cooperation should be made useful for identity management.

5.2. Relationship between controller and data subject

The controller and the data subject have divergent starting positions with regard to the available information. In particular the relationship between the controller and the data subject is characterized by an asymmetry of the available information. After identifying the information asymmetry, the relationship between the controller and the data subject should be analyzed with the game theory. With applying the game theory the economic perspective in the interaction between controller and data subject can lead to further findings for effective identity protection. Finally, the conflict of interest between the data subject and the controller has to be classified in order to define an appropriate mechanism for conflict resolution.

Information asymmetry. The preparation of the processing, the legitimization of the processing and the exercise of the data subject rights can be described as phases of the processing in the GDPR. The determination of phases of processing in the GPDR clarifies the different degrees of influence the controller and data subject have during the data cycle. In order to include interdisciplinary research results regarding the actions of the data subject and the controller in each phase the relevant regulations in the GDPR shall be demonstrated.

In the phase of preparing the processing, the decisions by the controller on the degree of implementing the principles of data processing based on Art. 5 para. 1 GDPR may already lead to an information asymmetry. This information asymmetry develops because the controller knows the details about the amount of collected personal data

and the detection possibilities out of profiles. In particular the controller chooses the technology for processing based on the required state of the art in Art. 25 GDPR, which is unknown to the data subject. The controller might even apply persuasive technologies that should encourage the consent and high period of use by the data subject [10]. It is in the economic interest of the controller to attract many users and encourage the data subject to disclose a large amount of personal data. It is also in the economic interest of the controller to encourage the consent by choosing a broadly formulated purpose for the processing, Art. 5 para. 1 b) GDPR. This broad purpose for processing is legitimized by consent or other legitimacy reasons, Art. 6, 7 GDPR. However, this information about the processing is only accessible for the data subject by reading the privacy policy diligently. And in some cases, it is even likely that the privacy policies are written in a way, that precisely meets the legal requirements by Art. 12, 13 GDPR and the information about the actual scope of the processing is missing. It can even occur that the privacy policies are incompliant with the requirements of Art. 12, 13 GDPR or they are formulated in a manner beyond what is required [38]. This could be if the privacy policy is drafted in a very abstract way, allowing a high degree of interpretation, or the privacy policy is very long, so that the data subject is likely to be overwhelmed by the information. Such privacy policies reinforce the information asymmetry between the controller and the data subject, because the possibilities to understand the risks of the processing by taking the privacy policies into account are limited. This illustrates that already in the phase of preparing the processing, that the relationship between the controller and the data subject is characterized by the higher level of information about the processing of the controller.

Moreover, the information asymmetry can be reinforced by the fact that processing is legitimated with consent or other grounds of legitimacy based on Art. 6, 7 GDPR. This is particularly the case, if the data subject does not read the data protection provisions. With regard to general terms and conditions it was argued in the "myth of the opportunity to read" [4], that a rational consumer does not read the terms and conditions. This seems also applicable to privacy policies. The research of *Acquisti* [1] verified the dominant interest of data subjects in a direct use of the service, which is perceived as gratification. So the decision-making process of the data subject is based on the interest on gratification rather than a rational decision that reflects the advantages and disadvantages of consenting to a service. This is an important fact to consider, as the right of informational self-determination requires the rational consent to generate *Ipse*-parts of personal identity. Thus, the information asymmetry between controller and data subject is reinforced by the privacy policies and the gratification interest to directly use the service.

Furthermore, if the data subject rights based on Art. 15–21 GDPR are applied the controller is required to realize the right. Once the processed personal data has been made transparent to the data subject, e.g. the right to be forgotten based on Art. 17 GDPR can be claimed in order to delete an *Ipse*-part of the personal identity. With these data subject rights the information asymmetry can be compensated to some extend. But still the information asymmetry remains if the controller is reserved to fully disclose the processed information. In particular, the German Federal Court of Justice (Decision from August 27, 2020, No. III ZB30/20) recently ruled against Facebook,

that it has to provide complete access to the Facebook account of the deceased daughter to the inheriting parents. This case illustrates the reluctance of data controller s to provide full access to the generated information on personal identities. So even by applying the data subject rights, the information asymmetry is likely not to be compensated. The controller still has the economic interest to keep a high amount of personal data and the generated profiles. In order to determine a mechanism for protecting personal identities the phases of data processing shall by analyzed from a game theoretical point of view.

Game Theory. The game theory allows the modeling of two players interacting with each other with different information about the game. The actions of the players depend on the opponent's previous action and can lead to a cooperative or defective action. It might occur that the opponent reacts reciprocal to cooperation with cooperation or reciprocal to defection with defection. Also the strategy-decision of a player can differ, so that the actions of the player refer to the first action of the game and ignore the last action of the opposing player to avoid reciprocal actions. The development of actions based on the information about the previous action changes with each iteration. Also the complexity of the game increases with the amount of iterations. In summary, the game theory consists of players, actions, payouts and information ("Players, Actions, Payoffs and Information-PAPI") with the assumption that the players act in order to maximize their output by rational choice [29]. The game theory in a business context refers to the outcome of financial loss or profit. In data protection law the personal information is subject to the actions of the data subject e.g. with providing the consent to the controller that certain personal information can be processed. In terms of game theory, these actions relate to the public good of personal information [13]. The public good of personal information is characterized by the fact that it cannot be consumed and is available to everyone. The public good of personal information is maintained by a high degree of cooperation and it is challenged by a high degree of defection. In order to protect the public good of personal information, it is of interest to reach a high amount of cooperation between the controller and the data subject.

The iterations between the controller and the data subject are prescribed by the GDPR. Thus, the phases of preparing the processing, the phase of legitimizing the processing and the phase of the data subject rights shall be subject to the game theoretical modeling. The phase of preparation for processing can be dominated by the economic interest of the controller to make profit through a limited investment into the state of the art (Art. 25 GDPR) of the processing. Such an action can be classified as defection by the controller. In particular, the controller might apply persuasive technologies that should seem for the data subject cooperative, but after diligent consideration, they serve the controller to encourage a quick consent [10]. Thus, these technologies seem as cooperation, but are actually a manipulated defective action by the controller. Moreover, the privacy policies are likely to be more in the interests of the controller rather than fully disclosing the true extent and risks of the processing [37]. However, this defective action by the controller can lead to the consent by the data subject due to the interest on gratification, as shown with *Acquisti* [1] above. This

action by the data subject can be classified as cooperation due to the trust in the lawfulness of the processing. If the data subject makes use of the data subject rights, the controller might choose a defective action on this request by realizing the data subject right in an unsatisfactory manner. Overall it can be summarized that the controller is likely to act in a defective manner, which conflicts with the interest of the data subject to cooperate on the public good of personal information. This conflict of interest between the controller and data subject regarding public good of personal information remains through the phases of data processing. Since this conflict is at the expense of the public good of personal information and the protection of personal identities, the conflict shall be characterized in order to identify a mechanism for resolution.

Classification of conflict. The conflict of interest regarding the protection of personal identities between the controller and data subject has to be characterized. In order to reach a high level of protection for the public good of personal information a mechanism should be defined that leads to a high degree of cooperative actions. In order to specify a mechanism for a high degree of cooperation, attention should be drawn to the theory of conflict. The model of conflict escalation by *Friedrich Glasl* might allow the determination of a possible mechanism to solve the conflict of interest [11]. Taking the nine stages of conflict escalation by *Glasl* [11] into account, the conflict is characterized by the second stage of "debate and polemic", so that each party wants to assert its point of view. In this stage of the conflict it can easily escalate further and end up in a "*win-lose*" solution at the expense of the public good of personal information. So a mechanism has to be identified in order to prevent further escalation. Such a mechanism should promote cooperation and sanction defective actions.

Consequently, the resolution of the conflict of interest between the controller and the data subject should include an environment of cooperation. This could be implemented by a mechanism for identity management that enables the parties to iteratively communicate and influence the identities in a cooperative manner. In particular, the handling of *Cookie*-consent includes such an iterative communication with the controller as the data subject can choose, which *Cookie* should be activated each time a website is accessed. This iterative communication enables the data subject to manage the personal identities for each website context. Thus, for each website context the data subject has the chance to manage the *Ipse*-parts of the personal identity by deciding whether they should be generated or not. Such iterative process allows the new formation of the relationship between the controller and the data subject. However, the data subject is still left in uncertainty regarding the profiles as *Ipse*-parts of the personal identity generated after the consent. The right of transparency based on Art. 15 GDPR might be a reasonable step to visualize the generated profiles and identities. In many cases, however, the data subject will have to bear the transaction costs for requesting the transparency on the generated profiles and personal identities. And such a request could lead to unsatisfactory disclosure of information by the controller regarding the profiles and personal identities. After all, the economic interests of controller s make cooperation with the data subject difficult, as the Facebook case above has shown. Therefore, communication with a high degree of iterations should serve as

a mechanism to resolve the conflict of interest to a "*win-win*"-solution. This should promote cooperation and protect the public good of personal information.

Conclusively, an "*identity management by design*"-mechanism could include a technical mediator that strengthens the position of the data subject. With a technical mediator the data subject gets the chance to influence the personal identities effectively. The controller could be held to implement a technical mediator in order to cooperate and ensure the protection of personal identities. Such a technical mediator would serve the public good of personal information and make defective actions more difficult. Thus, a technical mediator could provide a resolution of the conflicting interests between the controller and data subject by facilitating a cooperative environment.

5.3. Resolution with a technical mediator

The resolution of the conflict between the controller and data subject requires an environment that promotes cooperation. In game-theoretical models it was established that certain strategies encourage or discourage cooperation. In order to characterize the technical mediator, the environment for cooperation has to be defined. After defining the cooperative environment, the requirements of a technical mediator should be determined. With this technical mediator the personal identities should become negotiable and serve the notion of dynamic *Ipse*- and static *Idem*- identities.

Establishing a cooperative environment. The protection of personal identities in their *Ipse*-part requires an iterative and cooperative process. This process would widen the chances for pluralistic content of personal identities in their dynamic *Ipse*-part. A process with a high degree of iteration leading to cooperation was described by *Axelrod* in "The Evolution of Cooperation"[2] with the "TIT for TAT"-strategy.

This "TIT for TAT"-strategy describes that the chosen action whether to cooperate or to act defectively depends on the previous action. As the "TIT for TAT"-strategy starts with cooperation and punishes defective action with defection, it promotes cooperation [2]. It has the tendency to lead after several iterations to cooperation [2]. The advantage of the "TIT for TAT"-strategy is that it generates the reputation of cooperation [2]. In addition the "TIT for TAT"-strategy has the effect of blocking defective action [2]. Thus, the process for establishing a cooperative environment for dynamic personal identities needs a high degree of iteration and as a first step cooperation. This first step of the iterative process should be initiated by the controller by providing an "*identity management by design*" mechanism. With this mechanism the controller invites the data subject to cooperate. The "*identity management by design*" mechanism would allow the data subject to determine the different *Idem*- and *Ipse*-parts of identity. On this basis of a first cooperative action the chances to promote and maintain cooperation are high. A technical mediator could also be applied to promote cooperation by implementing a high degree of iteration and creating the necessary space for the realization of the fundamental rights in Art. 7, 8 CFR and protect the public good of personal information.

Technical mediator. The process of mediation is one method of alternative dispute resolution with the aim of creating value in a controversial conflict. With the European Mediation Directive, the specific requirements of the mediation process are regulated. In particular, it is defined that mediation is a structured process on a voluntary basis, to reach a settlement of the conflict with the assistance of a mediator, Art. 3 a) Mediation Directive [6]. This mediation process is lead by the third party of a mediator, who is guiding the parties in an effective, impartial, solution abstinent and competent manner, Art. 3 b) Mediation-Directive. Also the law recognizes technical mechanisms for mediation with the concept of online mediation [30]. This technical mechanism for mediation provides a multi-level communication process [3], [27], that allows the iterative exchange of interests promoting cooperation [32]. As the process of mediation in the online-version also provides the ethical standards of impartiality and voluntarily this can be adopted for the identity protection with a technical mediator. The process of mediation promotes cooperation of the parties by providing a high degree of iteration in order to reach a settlement. Since the mediator typically asks the parties to bring their personal interests into the process, the probability of cooperation increases.

These characteristics of mediation should be adopted for the protection of dynamic personal identities. The openness of the outcome of a mediation process enables the negotiation of personal identities to lead to pluralistic results. Thus, the mediation process enables dynamic identities and should be subject to a technical mechanism. Such a mechanism could be implemented by providing an *"identity management by design"* mechanism. This mechanism should include the values of a mediator that has to be impartial, solution abstinent and provide the parties an effective, structured process on a voluntarily basis to negotiate the personal identities. In particular, a technical mediator could be implemented with a specific interface design that allows the data subject to access the profiles of the identity. After having access to the personal identities, the data subject gets the opportunity to agree or disagree in order to negotiate the *Ipse*-parts of the personal identity. With the opportunity to choose between different *Cookie*-preferences, there is already a mechanism on a minimum level in the sense of *"identity management by design"*. Furthermore, an *"identity management by design"* mechanism should provide the circumstances to effectively agree or disagree and make use of the data subject rights.

In addition a technical mediator could be a crucial element to also provide protection against discrimination. The technical mediation would include the characteristics of a mediator being neutral and non-discriminatory. So the *"identity management by design"* mechanism would need instructions that guarantee dynamic, but non-discriminatory personal identities. These instructions should be embodied by a technical mediator. The technical mediator should recognize the race, origin and political orientation of a data subject and provide protection against discriminatory profiles. With such a technical mediator in an *"identity management by design"* mechanism discriminatory personal identities could be excluded from the generated profiles according to Art. 9 GDPR.

Thus, the *"identity management by design"* mechanism serves the contextual integrity of the data subject and provides an effective protection of dynamic identities.

From a technical point of view this concept could be implemented with a "dashboard" as proposed by *Raschke/Küpper/Drozd/Kirrane* [28]. With this "dashboard" the data subject is enabled to manage the rights in particular the right to information, the consent and the rights of the data subjects pursuant to Art. 15–21 GDPR. In order to protect personal identities in an online-context it would be desirable to extent such a "dashboard" with the transparency of personal identities in their *Ipse*- and *Idem*-parts. This would be possible by applying the access right based on Art. 15 GDPR. With such a mechanism, the iterative control on profiles as *Ipse*-parts of identities could raise awareness and enable the data subject to exercise the right to self-determination. In general, the GDPR already contains the rules to provide an iterative process in order to negotiate personal identities. This iterative process is defined in the GDPR by the phase of preparing the processing, the justification and the phase in which the rights of the data subject can be exercised (Fig. 2). This iterative process of negotiating personal identities is one possibility for an "*identity management by design*" mechanism that could be applied from a technical point of view.

The requirement to technically protect personal identities in their *Ipse*- and *Idem*-parts serves the implementation of the right of informational self-determination. Also the requirement of an *"identity management by design"* mechanism would be an incentive to controller s to review existing technical and organizational measurements. This would be a major step to solve the conflict of interest between the controller and the data subject with a mechanism promoting cooperation. If the "*identity management by design*" mechanism is implemented it could also be applied as a tool for risk minimization based on Art. 32 para. 2 GDPR. Furthermore the *"identity management by design"* mechanism could be matter of documentation and reduce the accountability of the controller, Art. 5 para. 2 GDPR.

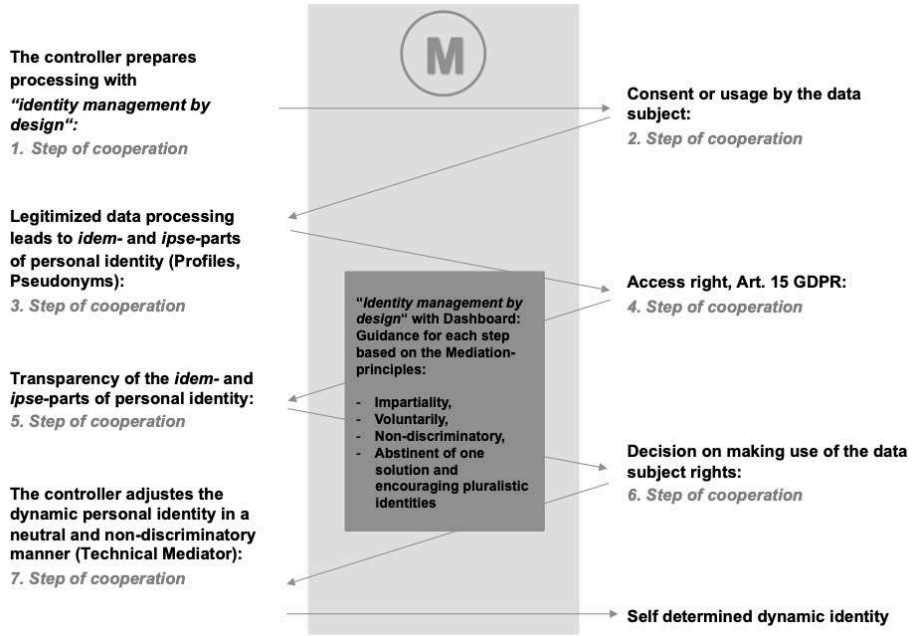

Fig. 2. Model of a "*identity management by design*"-concept with a technical mediator.

5.4. Technical mechanism for dynamic identities

The *Idem*- and *Ipse*-parts of personal identities require a mechanism in order to negotiate the personal identities. The concept of cooperation is part of the GDPR and therefore can also be applied for the protection of personal identities. The relationship between the controller and the data subject is characterized by information asymmetry. This information asymmetry already exists in the phase of the preparing the processing and continues after the data subject rights are exercised. The information asymmetry is also a part of a conflict of interest between the controller and the data subject. The conflict was analyzed by applying the game theory, which lead to the differentiation between cooperative and defective actions by the parties. With this analysis it was shown that the protection of the public good of personal information and personal identities requires a cooperative environment. Such an environment can be provided with an *"identity management by design"* mechanism that includes a technical mediator. The technical mediator would guarantee an iterative process that allows the negotiation of personal identities. With this process, the right of informational self-determination can be effectively exercised so that the personal identities in their *Idem*- and *Ipse*-parts can be realized. For this the mechanism of *"identity management by design"* should include a technical mediator.

6. Conclusion

The *"identity management by design"* mechanism as proposed would meet the principle of transparency based on Art. 5 sec. 1 a) GDPR. This mechanism would provide the data subject with an overarching perspective on the *Idem*- and *Ipse*-parts of personal identities. With the access and transparency rights based on Art. 13, 15 GDPR the generated personal identities of the data subject become accessible and negotiable. This enables the data subject to exercise iterative control regarding the *Ipse*- and *Idem*-parts of personal identities. Such an iterative control would provide further protection for users against generated profiles, as it would enable further self-determination in the online-context. This would require to make the pluralistic identities in the online-context accessible. With the technical method to provide transparency about the identities could be a "dashboard". Such a "dashboard" would serve the protection of personal identities according to the fundamental rights based on Art. 7, 8 CFR. With this technical mechanism for protection, the personal development would be enabled in the online-context in the same way as in the offline context. With an *"identity management by design"*-mechanism including a technical mediator the personal identities become legitimized by an iterative procedure. With a technical mediator, the process of mediation in its capacity of adding value may serve to protect identity. This procedure would directly reflect the concept of dynamic identities in the fundamental rights from Art. 7, 8 GRCh for the online context and provide further protection.

Thus, such a procedure with a technical mediator for the data subject would fulfill the concept of "legitimacy by procedure" [23]. In order to provide an effective incentive for controller the term *"identity management by design"* could be added into the wording of Art. 25 GDPR. Given its regulatory nature, this might lead to a higher acceptance than adding the term *"identity management by design"* in the existing recital 78. Since the definition of personal data based on Art. 4 para. 1 GDPR contains the notion of "dynamic identities", a corresponding technical protection of personal identities is a necessary paradigm shift in data protection law. Furthermore, the obligation for a cooperative *"identity management by design"* would balance the use of persuasion technologies in the era of Big Data. In conclusion the mechanism of *"identity management by design"* with a technical mediator would provide an ethical and human rights-based environment for the development and determination of personal identities.

References

1. *Acquisti, Alessandro*, Privacy in electronic commerce and the economics of immediate gratification – Proceedings of the 5th ACM conference on Electronic commerce, ACM 2004, pp. 21–29.
2. *Axelrod*, Robert, The Evolution of Cooperation, Cambridge M.A. 2006.
3. *Barnett, Jeremy/Treleaven, Philip*, Algorithmic Dispute Resolution—The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies, The Computer Journal 2017, pp. 399–408.
4. *Ben-Shahar, Omri*, The Myth of the 'Opportunity to Read' in Contract Law, ERCL 2009, pp. 1–28.
5. *Bernsdorff, Norbert/Borowsky, Martin*, Die Charta der Grundrechte der Europäischen Union – Handreichungen und Sitzungsprotokolle, Baden-Baden 2002.
6. Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters.
7. *Dürig, Markus/Fischer, Matthias*, Cybersicherheit in Kritischen Infrastrukturen, DuD 2018, pp. 211–213 (214).
8. *Eidenmüller*, *Horst*, Ökonomische und spieltheoretische Grundlagen von Verhandlung/ Mediation, in: Breidenbach/Henssler (Hrsg.), Mediation für Juristen, 1997, pp. 31–55.
9. *Erikson, Erik H.*, Identität und Lebenszyklus – Drei Aufsätze, 27. Auflage, Berlin 2015, pp. 150.
10. *Fogg, B. J.,* Computers as persuasive social actors, in: Persuasive Technology: Using Computers to Change What We Think and Do, pp. 89–120 (94).
11. *Glasl, Friedrich*, Konfliktmanagement – Ein Handbuch für Führungskräfte, Beraterinnen und Berater, 12. Auflage, Bern u.a. 2020, pp. 236.
12. *González Fuster, Gloria*, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Cham, Heidelberg 2014, pp. 256, 266–271
13. *Hermstrüwer, Yoan*, Informationelle Selbstgefährdung – zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung, München 2016, pp. 158.

14.Hildebrandt, Mireille, Smart technologies and the end(s) of law – Novel entanglements of law and technology, Cheltenham, UK/Northampton, MA, USA 2015
15.Hildebrandt, Mireille, Profiling and AmI, in: Rannenberg, Kai, Royer, Denis; Deuker, André, The Future of Identity in the information Society, Berlin/Heidelberg, 2009.
16.Hornung, Gerrit, Die digitale Identität – Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden 2005.
17.Jarass, Hans D., Kommentar, Charta der Grundrechte der EU, München 2016 Art. 7 GRC.
18.Keupp, Heiner, Identitätskonstruktionen – Das Patchwork der Identitäten in der Spätmoderne, Reinbek bei Hamburg 1999, pp. 99–103, 215.
19.Kieck, Annika, Der Schutz individueller Identität als verfassungsrechtliche Aufgabe – Am Beispiel des geschlechtlichen Personenstands, Berlin 2019.
20.Koops, E.; De Vries, Katja; Hildebrandt, Mireille, D7.14b: Idem-Identity and Ipse-Identity in Profiling Practices, FIDIS Report, 21. April 2009, pp. 28-33
21.Korsgaard, Christine M., Self-Constitution – Agency, Identity, and Integrity, Oxford 2009. pp. 35–37
22.Lippmann, Eric, Identität im Zeitalter des Chamäleons – Flexibel sein und Farbe bekennen, 2. Auflage, Göttingen/Bristol 2014.
23.Luhmann, Niklas, Legitimation durch Verfahren, 10. Auflage, Frankfurt am Main 2017.
24.Marsch, Nikolaus, Das europäische Datenschutzgrundrecht, Tübingen 2018, pp. 77, 209.
25.Maschmann, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, München 2018, Art. 88 DSGVO para. 14–16.
26.Nissenbaum, Privacy as contextual integrity, Wash. L. Rev. 2004, pp. 119.
27.Pretschner, Alexander/Walter, Thomas, Negotiation of Usage Control Policies - Simply the Best? – Third International Conference on Availability, Reliability and Security, IEEE 2008, pp. 1135–1136.
28.Raschke, Philip/Küpper, Axel/Drozd, Olha/Kirrane, Sabrina, Designing a GDPR-Compliant and Usable Privacy Dashboard, in: Hansen, Marit/Kosta, Eleni u.a. (Hrsg.), Privacy and Identity Management – The Smart Revolution, Berlin 2017, pp. 221–236.
29.Rasmusen, Eric, Games and information – An introduction to game theory, 4. Edition, Oxford, Malden, Victoria 2009, pp 182–185.
*30.*Regulation (EU) No 524/2013 of the European Parliament and the Council of 21 May 2013 on online dispute resolution for consumer disputes.
31.Ricœur, Paul, Oneself as another, Chicago 1994.
32.Schelling, Thomas C., The strategy of conflict, Oxford u.a. 1969.
33.Spindler, Gerald, Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung – Gutachten F zum 69. Deutschen Juristentag, in: Verhandlungen des 69. Deutschen Juristentages, München 212.
*34.*The Guardian: www.theguardian.com/news/series/cambridge-analytica-files (last accessed 2020/08/01).
35.Turkle, Sherry, Leben im Netz – Identität in Zeiten des Internet, Reinbek bei Hamburg 1999.
36.Watzlawick, Paul/Beavin, Janet H./Jackson, Don D., Menschliche Kommunikation – Formen, Störungen, Paradoxien, 13. Auflage, Bern 2016.
37.Windley, Phillip J., Digital identity – Unmasking identity management architecture (IMA), Beijing 2005.
38.Zander, Tim/Steinbrück, Anne/Birnstill, Pascal, Game-theoretical Model on the GDPR – Market for Lemons?, JIPITEC 2019, pp. 200.