netidee

PROJEKTE

Really Enforceable Solution to Protect End-users Consent & Tracking Decisions (RESPECTeD)

Soheil Human

Final Report (Endbericht) | Call 14 | Project ID Prj4625

Lizenz CC-BY-SA

1 Introduction

The *Advanced Data Protection Control* (ADPC) is a technical specification — and a set of sociotechnical mechanisms surrounding it — that can change the current practice of Internet-based personal data protection and consenting by providing novel and standardized means for the communication of privacy and consenting data, meta-data, information, requests, preferences, and decisions. ADPC supports humans in practicing their rights to privacy and agency by giving them more human-centric control over the processing of their personal data and consent. It helps the data controllers to improve their users' experiences and provides them with easy-to-adopt means to comply with the relevant legal and ethical requirements and expectations.

This technical report introduces the ADPC and describes the project that led to the development of the ADPC, i.e. the „Really Enforceable Solution to Protect End-user Consent & Tracking Decisions" (RESPECTeD) project, jointly conducted by the *Sustainable Computing Lab* at *the Vienna University of Economics and Business* (WU Wien) and the *NOYB – European Center for Digital Rights.* The project was led by Soheil Human and Max Schrems and was partially funded by the *netidee* funding program of *Internet Privatstiftung Austria – Internet Foundation Austria* under the grant number *prj4625*.

1.1 Personal Data Protection and Consenting as Human Rights

The protection of personal data is a human right [1, 2]. Therefore, personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned, or some other legitimate basis laid down by law" (Art. 8, Charter of Fundamental Rights of the European Union). Accordingly, empowering [3, 4] data subjects (e.g., users, customers), data controllers [5] (e.g., companies, organizations, service providers) and other involved actors to co-construct Human-centric, Accountable, Lawful, and Ethical (HALE) [6] data protection and consenting practices through sociotechnical systems should be considered an essential means for keeping (or making) our societies sustainable [7].

1.2 The Necessity of Advanced Mechanisms for Data Protection and Consenting Control Mechanisms

In our increasingly digital world, data in general, and personal data in particular, has become an important driver of digital innovation and economic growth [15, 16, 17], causing digitization and digital transformation in many sectors and application areas [18]. Keeping this transformation sustainable, however, has been a challenging mission [18]. Among others, the tension between providing personalized services — used in many cases as a basis for personalized advertisements — and respecting humans' privacy or agency has remained unresolved.

In the following, we argue that advanced Data Protection and Consenting Communication Mechanisms (like the ADPC) can contribute to resolving some of the most fundamental existing challenges concerning online privacy and consenting. Clearly, many different systemic, structural, technical, societal, eco- nomic, or political reasons are involved in the co-construction of the current and the future digital world. Therefore, the ADPC can only be helpful if it is well sup- ported by other sociotechnical means (e.g., complementary technical solutions, regulations, standards, policies, business models, or ethical frameworks).

i) Who is Controlling the Data Concerning Privacy and Consenting?

According to different legal frameworks such as the European General Data Protection Control (GDPR), data controllers are obliged to provide data sub- jects with privacy and consenting related information and — whenever needed — to obtain their consent or privacy-related decisions through lawful and ethical means. This is currently mainly practiced through the mechanisms that the data controllers provide (e.g., so-called “cookie banners”) [19]. Even if de- signed in transparent, understandable, ethical, and lawful manners—which is often not the case (see e.g., [20, 21, 22])—since the data-controllers design, develop, maintain, and provide these mechanisms (interfaces) on their sides (e.g., on their websites or apps), the data related to users’ privacy and consenting, e.g., their consent or decisions, remains solely under the control of the data con- trollers. This means that the data subjects do not even receive a copy of the data or any confirmation (e.g., receipts, see also [23]) related to their decisions (or related to the information that was provided to them). This puts the data subjects (i.e., humans, users, customers, etc.) in an inherently weak position. As described in the literature (e.g., [7]), humans have difficulties managing their online data protection and consenting from different cognitive, collective, and contextual perspectives. Without having access to data, empowering [4] humans with the expected cognitive, collective, or contextual supports [7] on their own side (on the user side) is almost impossible. The ADPC makes it possible to communicate such data in a bidirectional manner between different involved ac- tors, solving one of the most essential issues of the current practice of personal data processing on the Internet.

ii) Who is Controlling the Procedures concerning Data Protection and Consenting?

Along with controlling privacy and consenting data, data controllers currently fully control the data protection and consenting procedures. For example, the data controllers decide when the consent pop-ups appear or what kind of decisions should be communicated. This makes it possible for them to design the procedures in favor of their own interests. For example, consenting to all is the “default easy option” that can be performed through a consent banner, and withdrawing a previously given consent needs a time-consuming procedure using different forms that are sometimes hidden and hard to find. The ADPC makes it possible for the data subjects to have

autonomy and agency concerning the data protection and consenting procedures and, if needed, start the procedure themselves or modify the offered procedures. For example, a data subject can start the communication procedure themself by sending a withdrawal message to a data controller, or if a data controller sends different requests, the data subject can only answer to a subset of them. This provides a new balance between the data subjects and data controllers.

iii) Who is Controlling the User Interfaces and Designs Concerning Data Protection and Consenting?

In line with the previous two points, data controllers can currently decide on every detail of the user interfaces used in privacy and consent-obtaining mechanisms. This has increased the use of negative nudging mechanisms (also some- times called dark patterns) in the consent banners [24]. The ADPC brings privacy and consenting user interfaces to the user side, putting them under the control of the users and/or their trusted supporting actors (e.g., trusted family, friends, experts, NGOs, privacy-preserving technology developers, or browsers). In other words, complemented with other sociotechnical solutions, the ADPC can contribute towards ending (or at least reducing) the issue of dark patterns in relation to online privacy and consenting on the Internet — among others.

iv) Empowering Data Subjects, Empowering Data Controllers

The ADPC can empower users by involving them in controlling procedures, designs, and data management of online personal data processing. But, besides data subjects — that have difficulties dealing with online privacy and need to be empowered —, complying with different legal frameworks and developing various privacy management mechanisms is not an easy task for many data controllers as well (see, e.g., [25, 26]). Among others, developing consent mechanisms (e.g., so-called cookie banners) can be challenging, especially for smaller companies. The ADPC can enable novel means of communicating privacy and consenting with data subjects that might reduce the load of designing and maintaining some of the existing mechanisms, such as the cookie banners. Moreover, the current practice can be very disturbing for users. Considering that user experience is a significant factor for online service providers, replacing the banners with more advanced mechanisms that the ADPC can enable can be very beneficial for the companies [27].

1.3 About this document

Before describing the research and development conducted through the RESPECTeD[1] project (see sections 3—9), this document presents the Advanced Data Protection Control (ADPC) [13], a mechanism for the communication of data protection and consenting data, meta-data,

[1] https://respected.eu

information, requests, preferences, and decisions that can contribute toward a fundamental shift in the ways that personal data processing is practiced on the Internet: i.e., from a data-controller-centric practice to a data-subject-centric (i.e., a human-centric) practice. The aim here is to provide an interdisciplinary overview that is understandable for experts across different disciplines. The technical details of the communication specification can be found in the ADPC specification (see [13]) and have been reported in other academic publications.

Problem area: In recent years, a vast amount of research has shown that we have failed to protect end-users' right to privacy and agency (see, e.g., [8, 9, 10]). The consequences of this failure go way beyond the invasion of individuals' privacy and can negatively influence different aspects of our societies [11]. Therefore, tackling the problem of digital privacy and agency in a human-centric manner is a fundamental challenge of our time to protect humans' rights and keep/make our societies digitally sustainable [12].

While data controllers "control" most of the fundamental aspects of online privacy and consenting (see Section 2), data subjects are mostly left alone to deal with the difficulties and complexities of managing (and protecting) their online privacy and agency — a mission impossible.

The ADPC aims to tackle this important problem by contributing to a fundamental shift in the practice of online privacy and agency through enabling new communication mechanisms and, consequently, new assistive solutions — and ultimately by changing the control and power structures.

Approach: The ADPC was developed through a collaboration of an interdisciplinary team of computer scientists, social scientists, lawyers, activists, and practitioners, as a part of the RESPECTeD project1 led by the Soheil Human (Sustainable Computing Lab) and Max Schrems (NOYB – European Center for Digital Rights). In this document, we present the ADPC based on the questions that were identified through a set of interdisciplinary qualitative studies (a mixture of two focus groups and eight interviews) in which sixteen experts working on data protection and consenting topics with diverse expertise and backgrounds

(from computer science, natural science, law, social science and humanities) participated. The studies included other aspects that are not reported in this document. We hope that the provided questions-based narrative can make it easier for a non-technical audience to understand the bases of the ADPC.

Structure: In the next section, we will present the ADPC to an interdisciplinary audience through the questions identified in our qualitative studies. Sections 3 —9 include more details about the RESPECTeD project and our future plans.

2 Project Description

2.1 The Advanced Data Protection Control (ADPC)

The Advanced Data Protection Control (or the ADPC) is a technical specification (and the sociotechnical solutions surrounding it) for the communication of data protection and consenting data, meta-data, information, requests, preferences, and decisions. For example, the ADPC specification defines automated means for data subjects (e.g., website visitors) to 1) give or refuse consent for the specific purposes that the data controller describes, 2) withdraw any consent already given, as well as 3) object to processing for direct marketing purposes based on the data controller's legitimate interest. This enables the user to easily manage data protection decisions through the web browser and possibly customize how requests are presented and responded to (e.g., using a browser extension to import or specify lists of trusted websites). The result could be comparable to how websites ask for permission to access a webcam or microphone via a browser: the browser keeps track of the user's decisions on a site-by-site basis, ensures that the user gets a genuinely free choice (e.g., no dark pattern used), and puts the user in control over their decisions.

i) How does the ADPC work?

APDC specification defines a mechanism for expressing user decisions about personal data processing under the European Union's data protection regulations and similar regulations outside the EU. The mechanism functions by exchanging HTTP headers between the user agent and the web server or through an equivalent JavaScript interface. In the future, other protocols and technologies can also be used to transfer ADPC signals.

The mechanism serves as a means for users to give or refuse consent, with- draw any consent already given, and object to processing — among others. The mechanism provides an alternative to existing non-automated consent management approaches (e.g., cookie banners) and aims to reduce the efforts of the different parties involved regarding the protection and management of users' privacy.

ii) What are the legal foundations of the ADPC?

Besides the Charter of Fundamental Rights of the European Union, as it is mentioned in the ADPC specification [13], different legal frameworks such as the European Union's General Data Protection Regulation (GDPR) and ePrivacy Directive define rights and obligations around the processing of personal data[2]. The starting position of the GDPR is that the processing of personal data is only lawful if it has an appropriate legal basis; one basis being that "the data subject has

[2] The ADPC can also be used to manage privacy and consenting based on non-European legal frameworks.

given consent to the processing of his or her personal data for one or more specific purposes" (point (a) of Article 6(1) GDPR). Similarly, the ePrivacy Directive (in Article 5(3)) requires the user's consent when any data is stored on or retrieved from terminal equipment beyond what is strictly necessary. Moreover, when a data controller relies on legitimate interest as the legal basis for direct marketing, the user has an absolute right to object under Article 21(2) GDPR.

As website publishers often desire to process their visitors' personal data for purposes beyond what is necessary to serve the website and beyond what can be based on legitimate interest, a website operator often wants to ask whether the visitor consents to such processing. Such communication currently tends to be done via highly disruptive and repetitive interfaces contained in the web page itself (e.g., cookie banners) rather than through the web browser or other automated channels.

It is the user's choice how to communicate the exercise of GDPR rights to a data controller — the user could send an email, letter, or click a button on a website. In addition, technical means can be used:

Article 21(5) GDPR expressly provides that "the data subject may exercise his or her right to object by automated means using technical specifications". Recital 32 of the GDPR also makes clear that requesting and giving consent could take many forms, which "could include ticking a box when visiting an internet website, [or] choosing technical settings for information society ser- vices […]", as long as it satisfies the requirements such as being informed and unambiguous. Recital 66 of Directive 2009/136/EC, which updates the 2002 ePrivacy Directive, likewise states that "the user's consent to processing may be expressed by using the appropriate settings of a browser or other application". The proposed ePrivacy Regulation (2017/0003 (COD)) equally foresees automated means to communicate data subject preferences. Despite various le- gal provisions suggesting its validity, a standardized means for communicating GDPR rights has thus far been lacking.

iii) What does make the ADPC "Advanced"?

There have been other attempts to implement automatic privacy controls (such as the "Do Not Track"[3] (DNT) and its recently adapted revision the "Global Privacy Control"[4] (GPC) [29]). The ADPC is different because it has been designed to better integrate with the requirements of GDPR and the upcoming ePrivacy Regulation, as well as with other international laws:

[3] https://www.w3.org/TR/tracking-dnt/

[4] https://globalprivacycontrol.github.io/gpc-spec/

- The ADPC is domain-specific ('site specific'), so users can choose to tailor their interaction with different websites and data controllers.
- The ADPC allows opt-in (consent) and opt-out (objection) signals, whereas other signals were based on an opt-out framework.
- The ADPC allows domains to freely define a consent request or use a formulation standardized by industry groups (like the IAB's TCF specification). This makes ADPC open and interoperable with other systems.
- The ADPC allows general signals (like "reject all", "withdraw all", "object to all", "do not track", "do not sell"), specific signals (like consent to a specific request) and a combination of general and specific signals (like "reject all, but consent to requests 'x' and 'y"').
- The ADPC allows browsers, plugins, or operating systems to provide users with settings and logic that determines how requests are treated. This includes white- and blacklisting, industry-wide purposes, or logic like showing a request only when visiting a page regularly.
- The ADPC limits the (legal) fingerprinting surface by not sending any signal if a domain does not support The ADPC (and thereby publicly commits not to use the signal further), as well as sending different signals to different domains.

iv) Does the ADPC provide its own vocabulary?

The ADPC is not limited to any vocabulary (ontology). It can be used with different vocabularies depending on the sector, use case, legal requirements, etc. However, the ADPC can be complemented with standardized vocabularies, e.g., [30].

v) Who can start the procedure?

As discussed in the previous section, having the power of starting the procedure of communicating privacy and consenting data and decisions is an essential fac- tor that shapes the dynamics of online personal data processing. Privacy signals such as the DNT or the GPC make it possible for the users to send a single binary message to data controllers regardless of data controllers' consent obtaining mechanisms. Contrary to them, the current consent obtaining mechanisms, such as the cookie banners, give full control of starting the procedures

to data controllers. The ADPC, however, provides a bidirectional mechanism that al- lows each party to start the communication. For example, a data subject can send a withdrawal request without waiting for the data controllers to send a query, or a data controller can send a set of requests to a data subject to start the procedure — both are possible.

vi) Who decides about the user interface design?

A big advantage of the ADPC is that it brings the representation and decision- making mechanisms to the user-side. Depending on the implementation, the user themself, the browser companies, the plugin developers, or trusted actors can decide about (or design) the representation and decision-making mechanisms. As a result, the ADPC-based user interfaces, if designed in a Human- centric, Accountable, Lawful, and Ethical (HALE [6]) manner, can reduce (or eliminate) the usage of problematic nudging mechanisms (e.g., so-called dark patterns) in privacy-related solutions, by shifting the control from the data con- trollers to data subjects (or their trusted parties). Figure 1 shows an example of an ADPC-based graphical user interface (GUI) embedded in a browser under the control of a data subject.

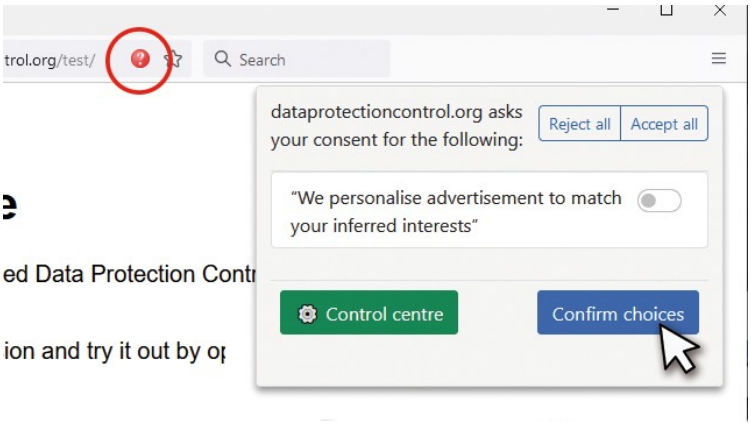

Figure 1: An example of a user-side ADPC-based GUI that is shown in a browser under the control of a data subject

vii) What about supporting users?

While bringing the privacy and consenting data to the user-side and empowering users through involving them in controlling the procedures and designs of personal data processing is certainly very important, as it is discussed in the literature [21, 28, 7], users— as human-beings—have limited cognitive capacities, knowledge, expertise, time, or motivation to manage their privacy alone. They need to be empowered [4] by sociotechnical means, such as the Personal Data Protection and Consenting Assistant Systems (PDPCAS) [7], that provide cognitive, collective, and contextual ([31, 32]) supports for them. Such systems can provide users with, e.g., automation tools, management tools, memorizing tools, trust assessment tools. Moreover, by being empowered to

control the procedures, users can be supported through white lists or black lists that can help them (or their agents, i.e., their PDPCASs) to interact with online ser- vices or make decisions regarding their privacy in easier manners. Without the ADPC (or similar mechanisms) development of PDPCASs or other supporting tools is almost impossible since such systems need to have access to privacy and consenting data and be involved in the procedures to function.

viii) Is the ADPC only limited to the web?

Currently, the ADPC supports HTTP and JavaScript, which means that it can be used in browsers and potentially web apps, mobile apps, and other solutions (from smart TVs to different IoT devices) that are based on these technologies. However, the ADPC aims to support other technologies as well in the future. For example, the Sustainable Computing Lab is currently leading a project that aims to bring the ADPC to IoT devices using Bluetooth.

ix) What is the difference between the ADPC and GPC or DNT?

Do Not Track (DNT) and Global Privacy Control (GPC) are binary HTTP header signals that are developed based on an approach to online privacy that is closer to California's legal framework, such as the California Consumer Privacy Act (CCPA). The ADPC, on the other hand, is a bidirectional advanced communication mechanism that can be used to communicate many different types of information and decisions related to privacy and consenting. The ADPC can be implemented in a way to produce binary signals similar to DNT or GPC, but it is not limited to that. While the ADPC was designed with European laws in mind, it is not limited to any legal frameworks and can be adapted to them.

x) What are the benefits for the data controllers?

As it was mentioned before, several benefits can be considered for the data con- trollers. Among others: 1) supporting the ADPC can show that companies respect their users' privacy and agency. This might be seen as a value-proposition (see e.g., [33]) for many of the companies and increase their trustworthiness. 2) Developing consent banners and maintaining them can be a costly and difficult task. The ADPC can reduce the load on data controllers in this regard. 3) The current consent banners are very distracting and reduce visitors' or customers' user experience. The ADPC can support the companies to eliminate them and improve their users' satisfaction and revenue (see, e.g., [27]).

xi) What about if someone misuses the ADPC?

Security and privacy measures have been considered in the development of the ADPC. For example, the ADPC is domain-specific (see above), which can highly reduce potentially problematic fingerprinting. But similar to other technologies, the ADPC might also be misused.

Depending on the sophistication of the specific implementations, the developers are expected to consider further privacy and security measures when implementing ADPC-based technologies. An analogy that can be helpful here is the email protocols (e.g., the Simple Mail Transfer Protocol, SMTP): while SMTP was designed by considering specific privacy and security measures, it does not prevent people from sending spams: other complementary solutions that provide different anti-spam techniques are expected to be included in the systems that implement SMTP. This is also the case with the ADPC; privacy and security measures and complementary solutions should be implemented along with the ADPC, depending on the application area, use case, and underlying technological systems.

2.2 Conclusion of Project Description

In this section, we used a set of questions identified through qualitative studies as a basis to introduce ADPC to interdisciplinary audiences that might not have deep technical expertise. We believe that the APDC has the potential to shift the power structure of the Internet, and it is essential to communicate its different aspects with a wide range of scientists, practitioners, activists, businesses, and policy-makers. We are also well aware that no technology alone can be impactful if other sociotechnical solutions will not support it. We call interdisciplinary communities that are working on privacy and consenting to work together to co-construct a next generation Internet that is Human-centric, Accountable, Lawful, and Ethical and realizes digital Sustainability as an essential aspect of our societies.

3 Workpackages

3.1 Workpackage 1 — Project Management

This workpackage included all our efforts to ensure the project's smooth development. Agile project management, together with regular consortium meetings, monitoring, and controlling were used to lead to successful project results.

3.2 Workpackage 2 — Standard Development

In this workpacakge, we developed the Advance Data Protection Control or ADPC, which is a technical specification (and its surrounding sociotechnical mechanisms) for the communication of data protection and consenting data, requests, and decisions. The workpackage, included literature research, internal workshops, communication and feedback sessions with a wide range of interdisciplinary experts that all led to the development, evaluation (together with WP4), and improvement of the developed specification.

3.3 Workpackage 3 — Plugin Development

As a proof of concept, we developed two pieces of software: 1) a browser plugin, 2) a server-side software. The developed software can support data controllers to adopt ADPC. They can also help users, policymakers, and other interdisciplinary experts to better understand the ADPC and its concepts and functionalities.

3.4 Workpackage 4 — Evaluation

After the development of the first version of the specification, we contacted several interdisciplinary experts. Based on their evaluation and feedback, we improved the ADPC specification. Moreover, we conducted focus group studies to compare the ADPC and the GPC to evaluate the developed specification based on a comparison with the other existing open specification.

3.5 Workpackage 5 — Dissemination

We had several dissemination activities to introduce the ADPC to a wide range of experts, among others:

- We co-created the W3C consent community group.
- We presented the ADCP at the CPDP Computers, Privacy and Data Protection conference in Brussels.
- We developed the ADPC website, which includes different text and multimedia content about the ADPC.
- We wrote different documentations and scientific publications regarding the project.
- We also have created partnership with different universities, organizations, and companies to develop the ADPC and ADPC-based solutions in the future.

4 List of Project Results

1	*Projektzwischenbericht*	*NA*	*NA*
2	**Project final report**	CC-BY Sharelike-3.0 AT	https://www.netidee.at/respected

3	**Entwickler_innen-DOKUMENTATION** (Documentation for the developers)	CC-BY Sharelike-3.0 AT	http://dataprotectioncontrol.org also https://github.com/Data-Protection-Control
4	**Anwender_innen-DOKUMENTATION** (documentation for the users)	CC-BY Sharelike-3.0 AT	http://dataprotectioncontrol.org/
5	**Project Summary**	CC-BY Sharelike-3.0 AT	https://www.netidee.at/respected
6	Documentation regarding the sustainability of the project results (see Section eight and nine of the final report)	CC-BY Sharelike-3.0 AT	https://www.netidee.at/respected
7	**A specification for communication of the end-users online privacy decisions**	MPL-2.0 license	https://github.com/Data-Protection-Control
8	**A browser plugin which works based on the developed standard (PoC for the data subjects)**	MPL-2.0 license	https://github.com/Data-Protection-Control
9	**A server side software (plugin) that works based on the developed standard (PoC for the data controllers)**	MPL-2.0 license	https://github.com/Data-Protection-Control
10	**An academic manuscript about ADPC**	preprint will be released as open access document, CC-BY-SA	epub.wu.ac.at

5 Application of Project Results in Practice

Different websites have already adopted the ADPC. Some of the Consent Management Platforms are working on including the ADPC in their solutions. A group of open-source developers is developing a WordPress plugin based on the ADPC. The development of other solutions based on the APDC is in progress. For example, we are developing the ADPC-IoT to bring the ADPC to the digital world beyond the web. We are also in contact with different data controllers to adopt the ADPC on their solutions or websites.

6 Public Relation Activities and Networking

The ADPC was presented in different workshops and conferences, such as the 2022 International Workshop on Privacy Engineering (IWPE'22), Co-located with the 7th IEEE European Symposium on Security and Privacy (EuroS&P), in Genoa (Italy) where we won a best paper presentation award. We presented the ADPC at Brussels's CPDP Computers, Privacy, and Data Protection conference. We had many meetings with policymakers, government and international bodies, scientists, activists, and companies regarding the ADPC. We have been writing academic and policy documents about the ADPC, and together with the W3C consent community group, we are advocating the ADPC to different communities.

7 Project Website

The project website: https://www.respected.eu

The ADPC website: https://www.dataprotectioncontrol.org

8 Planed Activities After the Netidee Project

We are working on the ADPC-IoT and aim to apply the ADPC in different real-world application areas. Moreover, we are in contract with different stakeholders to further push the adoption of the ADPC.

9 Proposals for Further Development by/through Third Parties

Different Consent Management Platforms (CMPs), data controllers, publishers, and organizations are interested in (and working on) adopting the ADPC. The W3C consent community group is working on different ADPC-based use cases.

10 Acknowledgements

On behalf of the ADPC core team, we acknowledge all people who contributed to the development of the ADPC. Many different colleagues and friends from the Vienna University of Economics and Business, Sustainable Computing Lab, NOYB, W3C community groups, various data protection boards and authorities, universities and research institutions, NGOs, parliaments and governments, international organizations, standardization bodies, journals and news agencies, open-source developers and communities, and companies supported this project by providing us with their input and feedback. We are very thankful for all these contributions. The ADPC was partially funded by netidee program of the “Internet Privatstiftung Austria – Internet Foundation Austria” (grant number prj4625). We appreciate this support.

11 References

[1] Gloria Gonz´alez Fuster. The emergence of personal data protection as a fundamental right of the EU, volume 16. Springer Science & Business, 2014.

[2] Stefano Rodot`a. Data protection as a fundamental right. In Reinventing data protection?, pages 77–82. Springer, 2009.

[3] Rainer Alt, Soheil Human, and Gustaf Neumann. End-user empowerment in the digital age. In Proceedings of the 53rd Hawaii International Confer- ence on System Sciences, Hawaii, United States, 2020. None.

[4] Soheil Human, Rita Gsenger, and Gustaf Neumann. End-user empower- ment: An interdisciplinary perspective. pages 4102–4111, Hawaii, United States, 2020.

[5] Fabian Burmeister, Paul Drews, and Ingrid Schirmer. A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation. Hawaii International Conference on System Sciences 2019 (HICSS-52), January 2019.

[6] Soheil Human. THE HALE WHALE: A Framework for the Co-creation of Sustainable, Human-centric, Accountable, Lawful, and Ethical Digital Sociotechnical Systems. Sustainable Computing Paper Series, (2022/01), 2022.

[7] Soheil Human, Rainer Alt, Hooman Habibnia, and Gustaf Neumann. Human-centric Personal Data Protection and Consenting Assistant Sys- tems: Towards a Sustainable Digital Economy. In Proceedings of the 55th Hawaii International Conference on System Sciences, pages 4727–4736, Hawaii, USA, 2022. University of Hawaii.

[8] C´elestin Matte, Nataliia Bielova, and Cristiana Santos. Do cookie banners respect my choice?: Measuring legal compliance of banners from iab eu- rope's transparency and consent framework. In 2020 IEEE Symposium on Security and Privacy (SP), pages 791–809. IEEE, 2020.

[9] Shoshana Zuboff. Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, 30(1):75–89, 2015.

[10] Jim Isaak and Mina J Hanna. User data privacy: Facebook, cambridge analytica, and privacy protection. Computer, 51(8):56–59, 2018.

[11] Soheil Human, Gustaf Neumann, and Markus F. Peschl. [How] can pluralist approaches to computational cognitive modeling of human needs and values save our democracies? Intellectica, 70:165–180, 2019.

[12] Soheil Human, Gustaf Neumann, and Rainer Alt. Human-centricity in a Sustainable Digital Economy. In Hawaii International Conference on System Sciences (HICSS-54), Hawaii, USA, 2021.

[13] Soheil Human, Max Schrems, Alan Toner, Gerben, and Ben Wagner. Ad- vanced Data Protection Control (ADPC). Sustainable Computing Reports and Specifications 2021/01, Vienna University of Economics and Business (WU Wien), Vienna, 2021.

[14] Soheil Human. Data protection and consenting communication mecha- nisms. Sustainable Computing Paper Series, (2022/01), 2022.

[15] Thorhildur Jetzek, Michel Avital, and Niels Bjorn-Andersen. Data-driven innovation through open government data. Journal of theoretical and ap- plied electronic commerce research, 9(2):100–120, 2014.

[16] James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, Angela Hung Byers, et al. Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute, 2011.

[17] Alina Sorescu. Data-driven business model innovation. Journal of Product Innovation Management, 34(5):691–696, 2017.

[18] Soheil Human, Gustaf Neumann, and Rainer Alt. A Call for Interdis- ciplinary Research on Applied Human-centricity in a Sustainable Digital Economy. pages 4695–4696, Hawaii, USA, 2022.

[19] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy. arXiv preprint arXiv:1808.05096, 2018.

[20] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (un) informed consent: Studying gdpr consent notices in the field. In Proceedings of the 2019 acm sigsac conference on computer and communi- cations security, pages 973–990, 2019.

[21] Soheil Human and Florian Cech. A Human-Centric Perspective on Digital Consenting: The Case of GAFAM. In Alfred Zimmermann, Robert J. Howlett, and Lakhmi C. Jain, editors, Human Centred Intelligent Systems, Smart Innovation, Systems and Technologies, pages 139–159, Singapore, 2021. Springer.

[22] Cristiana Santos, Nataliia Bielova, and C´elestin Matte. Are cookie ban- ners indeed compliant with the law? deciphering eu legal requirements on consent and technical means to verify compliance of cookie banners. arXiv preprint arXiv:1912.07144, 2019.

[23] Vitor Jesus. Towards an accountable web of personal information: The web-of-receipts. 8:25383–25394, 2020.

[24] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark patterns after the gdpr: Scraping consent pop-ups and demon- strating their influence. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pages 1–13, 2020.

[25] Daniel Mikkelsen, Henning Soller, Malin Strandell-Jansson, and Marie Wahlers. Gdpr compliance since may 2018: a continuing challenge. McK- insey & Company, 22, 2019.

[26] Monika Tsaneva et al. Challenges of gdpr compliance in consumer financing companies. In Conferences of the department Informatics, number 1, pages 103–115. Publishing house Science and Economics Varna, 2019.

[27] Flavia Salutari, Diego Da Hora, Matteo Varvello, Renata Teixeira, Vas- silis Christophides, and Dario Rossi. Implications of the multi-modality of user perceived page load time. In 2020 Mediterranean Communication and Computer Networking Conference (MedComNet), pages 1–8. IEEE, 2020.

[28] Soheil Human, Gustaf Neumann, and Markus F. Peschl. [How] can pluralist approaches to computational cognitive modeling of human needs and values save our democracies? Intellectica, 70:165–180, 2019.

[29] Sebastian Zimmeck and Kuba Alicki. Standardizing and implementing do not sell. In Proceedings of the 19th Workshop on Privacy in the Electronic Society, pages 15–20, 2020.

[30] Harshvardhan J Pandit, Axel Polleres, Bert Bos, Rob Brennan, Bud Brueg- ger, Fajar J Ekaputra, Javier D Fern´andez, Roghaiyeh Gachpaz Hamed, El- mar Kiesling, Mark Lizar, et al. Creating a vocabulary for data privacy. In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems", pages 714–730. Springer, 2019.

[31] Niklas Kirchner, Soheil Human, and Gustaf Neumann. Context-sensitivity of informed consent: The emergence of genetic data markets. In Workshop on Engineering Accountable Information Systems. European Conference on Information Systems-ECIS, 2019.

[32] Soheil Human and Mandan Kazzazi. Contextuality and intersectionality of e-consent: A human-centric reflection on digital consenting in the emerging genetic data markets. In 2021 IEEE European Symposium on Security and Privacy Workshops (EuroSPW), pages 307–311, 2021.

[33] Howard Simkevitz. Why privacy matters in health care delivery: a value proposition. In 2009 World Congress on Privacy, Security, Trust and the Management of e-Business, pages 193–201. IEEE, 2009.