

# GDPR Reality Check – Claiming and Investigating Personally Identifiable Data from Companies

Fatemeh Alizadeh, *University of Siegen*  
Timo Jakobi, *University of Siegen*  
Alexander Boden, *Fraunhofer Institute*  
Gunnar Stevens, *University of Siegen*  
Jens Boldt, *University of Siegen*

## Abstract

Today, more personal data than ever before is being collected and stored by companies of all types for a wide variety of purposes. The General Data Protection Regulation (GDPR) aims to strengthen the rights of consumers by providing them with tools for controlling data collection and processing. While companies are now subject to legal obligations, precedent cases are still missing. At the same time, it remains unclear how the right to access data can be concretely implemented in practical and technical terms. Our study intends to address this problem by investigating the case of loyalty card providers—an established branch that collects the purchase data of users in exchange for discounts. For our study, we asked 13 households to request their personal data from their respective loyalty program providers. Based on interviews, we investigate the expectations of these users of the GDPR and the right to access data. Furthermore, we analyze the currently implemented process of claiming and receiving data as well as the sense-making of said data by the users. Based on our analysis, we make the following contributions: We shed light on what users know about and expect from the GDPR, particularly concerning the right to access, we report user expectations regarding the process to claim access to data and the data archives provided, and finally, we also show why also companies could benefit from actively designing the data take-out to demonstrate their data collection practices.

## Paper link:

<https://ieeexplore.ieee.org/document/9229806>

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

*USENIX Symposium on Usable Privacy and Security (SOUPS) 2021*. August 8 – 10, 2021, Vancouver, B.C., Canada.

## References

- [1] Abras, C. et al. 2004. 1. Introduction and History. (2004), 14.
- [2] Acharya, A.S. et al. 2013. Sampling: why and how of it? *Indian Journal of Medical Specialities*. 4, 2 (Jul. 2013). DOI:<https://doi.org/10.7713/ijms.2013.0032>.
- [3] Adams, A. et al. 1997. Making Passwords Secure and Usable. *People and Computers XII* (London, 1997), 1–19.
- [4] Angulo, J. et al. 2015. Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (New York, NY, USA, 2015), 1803–1808.
- [5] Bellotti, V. and Edwards, K. 2001. Intelligibility and Accountability: Human Considerations in Context-Aware Systems. *Human-Computer Interaction*. 16, 2–4 (Dec. 2001), 193–212. DOI:[https://doi.org/10.1207/S15327051HCI16234\\_05](https://doi.org/10.1207/S15327051HCI16234_05).
- [6] Betzing, J.H. et al. 2019. The impact of transparency on mobile privacy decision making. *Electronic Markets*. (Feb. 2019). DOI:<https://doi.org/10.1007/s12525-019-00332-3>.
- [7] Boren, T. and Ramey, J. 2000. Thinking aloud: reconciling theory and practice. *IEEE Transactions on Professional Communication*. 43, 3 (Sep. 2000), 261–278. DOI:<https://doi.org/10.1109/47.867942>.
- [8] De Hert, P. et al. 2018. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*. 34, 2 (Apr. 2018), 193–203. DOI:<https://doi.org/10.1016/j.clsr.2017.10.003>.
- [9] EUR-Lex - 32016R0679 - EN - EUR-Lex: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Accessed: 2020-03-15.
- [10] Fischer, B. Bonuskarten: Das System Payback.
- [11] Jakobi, T. et al. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 2, (Dec. 2018), 1–28. DOI:<https://doi.org/10.1145/3287049>.
- [12] Jakobi, T. et al. 2019. It Is About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering. *ACM Transactions on Computer-Human Interaction*. 26, 1 (Jan. 2019), 2:1–2:44. DOI:<https://doi.org/10.1145/3281444>.
- [13] Jakobi, T. et al. 2018. Privacy-By-Design für das Connected Car: Architekturen aus Verbrauchersicht: Eine nutzerorientierte Diskussion. *Datenschutz und Datensicherheit - DuD*. 42, (Nov. 2018), 704–707. DOI:<https://doi.org/10.1007/s11623-018-1029-7>.
- [14] Kang, R. et al. 2015. “My data just goes everywhere”: user mental models of the internet and implications for privacy and security. *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada, Jul. 2015), 39–52.
- [15] Kizilcec, Rene. F. 2016. “How much information?”: Effects of transparency on trust in an algorithmic interface. *CHI 2016, May 7–12, 2016, San Jose, CA, USA*, 39–52. ACM 978-1-4503-3362-7/16/05...\$15.00
- [16] Mayring, P. 2010. Qualitative Inhaltsanalyse. *Handbuch Qualitative Forschung in der Psychologie*. G. Mey and K. Mruck, eds. VS Verlag für Sozialwissenschaften. 601–613.

- [17] Medien zur DSGVO: Die Berichterstattung vor und seit dem Stichtag im Vergleich: <https://www.springerprofessional.de/en/medien-zur-dsgvo-die-berichterstattung-vor-und-seit-dem-stichtag/16515496>. Accessed: 2020-03-15.
- [18] Morey, T. et al. 2015. Customer Data: Designing for Transparency and Trust. *Harvard Business Review*.
- [19] Olausson, M. 2018. User control of personal data : A study of personal data management in a GDPR-compliant graphical user interface. (2018).
- [20] Raschke, P. et al. 2018. Designing a GDPR-Compliant and Usable Privacy Dashboard. *Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers*. M. Hansen et al., eds. Springer International Publishing, 221–236.
- [21] Reidenberg, J.R. et al. 2015. Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. *Berkeley Technology Law Journal*. 30, (2015), 39.
- [22] Schaub, F. et al. 2018. A Design Space for Effective Privacy Notices\*. *The Cambridge Handbook of Consumer Privacy*. E. Selinger et al., eds. Cambridge University Press, 365–393.
- [23] Spagnuolo, D. et al. 2019. Accomplishing Transparency within the General Data Protection Regulation: *Proceedings of the 5th International Conference on Information Systems Security and Privacy* (Prague, Czech Republic, 2019), 114–125.
- [24] Stevens, G. et al. 2014. Mehrseitige, barrierefreie Sicherheit intelligenter Messsysteme. *Datenschutz und Datensicherheit - DuD*. 38, 8 (Aug. 2014), 536–544. DOI:<https://doi.org/10.1007/s11623-014-0180-z>.
- [25] Tolmie, P. et al. 2016. “This has to be the cats”: Personal Data Legibility in Networked Sensing Systems. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (San Francisco, California, USA, Feb. 2016), 491–502.
- [26] Voigt, P. and Bussche, A. von dem 2018. *EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch*. Springer-Verlag.
- [27] Wong, J. and Henderson, T. 2018. How Portable is Portable?: Exercising the GDPR's Right to Data Portability. *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers - UbiComp '18* (Singapore, Singapore, 2018), 911–920.
- [28] 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.