A PRACTICAL GUIDE TO

DAVID CAUCHI

ITSM PRESS

A Practical Guide to GDPR

A Practical Guide to GDPR

ISBN Paperback: 9781912651306
ISBN eBook: 9781912651313

ITSM Press is the wholly owned publishing imprint of ITSM Shop Ltd.

Other ITSM Press Publications:

A Concise Introduction to ISO 14001:2015
A Concise Introduction to GDPR
A Concise Introduction to ISO/IEC 27001:2013
Service Management: It’s All About the People
PM4A: Project Management for All

ITSM Shop Ltd
95 Duxford Road, Whittlesford, Cambs, CB22 4NJ, UK
+44 (0) 3333 445 286
customerservices@itsmshop.co.uk
www.itsmshop.co.uk/

Table of contents

5.
Consent

Lot of emphasis is being put on consent as a legal basis to process personal data. However, it should be clarified at the outset that consent, albeit being amplified in the GDPR, is only one of the options and not the only one. Other possible options for processing will be dealt with in section 6 of this guide.

The GDPR lays down prescriptive rules on the elements that a valid consent should have. Consent should be a **freely given, specific, informed** and **unambiguous** indication of the data subject which denotes agreement to the processing of personal data relating to him or her. Such consent is to be given by means of a **statement or clear affirmative action**. An individual has the right to **withdraw** consent at any time.

Consent Do's

- ✓ Offer a genuine choice
- ✓ Clearly distinguish consent from other matters
- ✓ Use clear and plain language
- ✓ Be able to demonstrate consent
- ✓ Give a detailed and granular choice for different purposes
- ✓ Put the data subject in control
- ✓ Provide a concise and layered notice
- ✓ Allow individuals to reconsider or refresh their choices through a privacy dashboard
- ✓ Facilitate withdrawal of consent

Consent Don'ts

- × Silence and inactivity
- × Pre-ticked boxes
- × Power imbalance (e.g. where it is clear that disadvantaged position for individuals)
- × Consent tied up to a contract or conditions
- × Consent for mandatory processing
- × Consent based on incentives or adverse consequences
- × Bundled consent for various purposes
- × Ambiguous or unclear information
- × Tiring and disruptive notices

Example 5.1 - Consent wording

‘By accepting our terms and conditions you are granting your unconditional and irrevocable consent to the processing of your personal data, including possible disclosure to third parties…’

The example given above clearly lacks the elements of a valid consent and contains most of the possible pitfalls that controllers should avoid when obtaining consent under GDPR.

5.2. Explicit consent

There are situations where the GDPR requires such consent to be explicit in order to legitimise the processing of personal data. This occurs when processing involves serious risks for data subjects or where a high level of control is necessary. Where consent is used as a basis to process special categories of personal data, to carry out international transfers or for automated decision making and profiling, such consent has to be explicit. In these cases, consent should be obtained separately and distinctly from other processing operations.

5.3. Consent for children

The GDPR makes special provisions for children’s consent when acceding to information society services. The law requires a child to be at least 16 years of age in order to be capable to give consent for such services, without any parental intervention. However, the GDPR allows Members States to lower such age to a minimum of 13 years. For other situations involving children’s consent, the applicable national provisions establishing the age of consent will have to be considered.

Author

David Cauchi is a seasoned data protection expert, having worked in the field for more than 14 years. After graduating in Management and Banking & Finance, with Honours in Management at the University of Malta in 2003, David joined the Maltese Data Protection Authority. Since then, he formed part of the technical team, where he is currently serving as Head Compliance.

Throughout all these years, David has developed a level of expertise in data protection matters, particularly in handling complaints, carrying out inspections and audits, dealing with cross-border issues, including international data transfers, providing guidance and raising awareness on data protection to the various sectors, including banking and financial services, online gaming, employment, and the public at large.

He also represents the Information and Data Protection Commissioner in various Data Protection fora and meetings organised by EU Institutions. He is actively involved in the Coordinated Supervision of EU large-scale information systems, such as Europol, Schengen (SISII), Visa (VIS), Eurodac and Customs (CIS). David is currently serving his first term as Chair of the SIS II Supervision Coordination Group, having been elected in November 2017, after serving as Vice-Chair for the previous four years.

He is often invited to participate as expert speaker in conferences and seminars on GDPR.

More information about the author is available on
https://www.linkedin.com/in/cauchi-david-49090b5