Global Data and Cyber Handbook - EU

Information Requirements, Data Subject Rights, Accountability and Governance

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What information needs to be included in a privacy notice to data subjects?

*Last review date: January 2025*

☒   the identity and the contact details of the controller and, where applicable, of the controller's representative  
☒   the contact details of the data protection officer, where applicable  
☒   the purposes of the processing for which the personal data is intended  
☒   the legal basis for the processing  
☒   the legitimate interests pursued by the controller or by a third party if processing is based on the legitimate interests ground  
☒   the recipients or categories of recipients of the personal data, if any  
☒   information regarding data transfers to third countries, where applicable, and reference to appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available  
☒   the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period  
☒   the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc.  
☒   the existence of the right to withdraw consent if processing is based on consent  
☒   the right to lodge a complaint with a supervisory authority  
☒   whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data  
☒   if applicable, information regarding automated decision making, including profiling  
☒   other

The requirement to include information in the privacy notice on the categories of personal data concerned and the source from which the personal data originates only apply if the data is collected indirectly.

The obligation to provide information on the existence of data subjects’ rights requires the provision of information on the existence of all data subjects’ rights, (i.e., the right to access, rectification, erasure, data portability, restriction on processing, objection to processing) with a summary of what the right involves and how the data subject can take steps to exercise it and any limitations on the right.

The privacy notice must explain that data subjects have the right to withdraw consent at any time if the processing is based on consent.

Providing information on the security provided to the data is good practice, but not mandatory.

# Do data subjects have specific privacy rights that must be operationalized?

*Last review date: January 2025*

Yes

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

☒   right to access the data subject's own personal data

☒   right to rectify/correct the data subject's own personal data where inaccurate or incomplete

☒   right to erasure of personal data

☒   right to restrict data processing

☒   right to data portability

☒   right to object to the processing of personal data

☒   right to withdraw consent

☒   other

The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject;  right to transparent information (which, in practice, is an obligation of the data controller to provide such transparent information about its data processing activities).

We also note, pursuant to recital (27) of Regulation (EU) 2016/679 (GDPR), that although the GDPR does not apply to deceased persons, Member States of the European Union may establish local rules regarding the processing of personal data of deceased persons (e.g., specific rights that close relatives may exercise relative to such deceased persons’ personal data). Furthermore, the data subject also has the right to lodge a complaint with the competent data protection supervisory authority and make civil claims against the data controller and/or the data processor regarding alleged breaches of the GDPR; however, such rights cannot be operationalized, because the data subject does not exercise them by way of contacting the data controller or the data processor.

# Are there accountability and governance requirements?

*Last review date: January 2025*

Yes

There are accountability and governance requirements to:

☒   take privacy by default and design measures for all processing of personal data

☒   perform and document data protection impact assessments (DPIAs) for high-risk processing:

☒   maintain a record of processing activities

☒   implement appropriate measures to comply with data privacy and cybersecurity

☒   demonstrate compliance with data privacy and cybersecurity

☒   identify a specific individual as the data privacy contact for data subject or data protection authority inquiries

☒   provide training to employees

☒   audit or supervise data processors

☒   appoint a local representative in the jurisdiction (if the controller or processor is not located in the jurisdiction)

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.