SmartSuite

Framework / Privacy / Global Privacy Regulations

UK GDPR (retained Regulation (EU) 2016/679)

The UK GDPR is Regulation (EU) 2016/679 as it forms part of UK law, applying since December 31, 2020 and amended by the Data (Use and Access) Act 2025.



What it is

The UK GDPR is Regulation (EU) 2016/679 as it forms part of UK law under section 3 of the European Union (Withdrawal) Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419, made February 28, 2019). It has applied since IP completion day, December 31, 2020 at 11.00 p.m., to controllers and processors established in the UK and, under Article 3(2), to those outside it that offer goods or services to people in the UK or monitor their behavior there. It is enforced by the Information Commission, which replaced the Information Commissioner on September 30, 2026.

At a glance

PUBLISHER UK Parliament and government (SI 2019/419); regulator: the Information Commission (until September 30, 2026 the Information Commissioner)	TYPE Regulation	VERSION UK GDPR: Regulation (EU) 2016/679 as it forms part of UK law, as amended by SI 2019/419 and the Data (Use and Access) Act 2025
EFFECTIVE December 31, 2020, 11.00 p.m. (IP completion day); Data (Use and Access) Act 2025 amendments from February 5, 2026	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION United Kingdom	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: legislation.gov.uk/eur/2016/679/contents

Why it matters

- **A named set of principles** Article 5(1) lists lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation and integrity and confidentiality, with accountability in Article 5(2).
- **Six lawful bases plus one** Article 6(1) lists consent, contract, legal obligation, vital interests, public task and legitimate interests, and since February 5, 2026 recognized legitimate interests in point (ea).
- **Clock-based rights** Articles 12 and 12A give a controller one month from the relevant time to act on a request, extendable by two further months where requests are complex or numerous.
- **A fixed breach clock** Article 33 requires notification to the Commission without undue delay and where feasible within 72 hours of becoming aware of a breach.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports UK GDPR

Records of Processing (Article 30)

Maintain each activity's purpose, lawful basis, categories, recipients, transfers and retention, with the Article 30(5) exemption decision recorded where relied on.

Lawful Basis and Annex 1 Register

Record the Article 6 basis for each purpose, including recognized legitimate interests and the Annex 1 condition, and the Article 9 condition for special category data.

Data Subject Request Clock

Track each request with its relevant time, one-month deadline, any two-month extension notice, paused periods and the reasonable and proportionate search carried out.

Impact Assessments and Automated Decisions

Run Article 35 assessments and record significant automated decisions with the Article 22C safeguards: information, representations, human intervention and contest.

Breach Notification Clock

Log the time of awareness, the 72-hour Article 33 deadline, the notification to the Commission and the communication to individuals.

Transfer Register

Record each restricted transfer under Article 44A, the route relied on, the data protection test assessment and the safeguards in Third Party Risk Management.

Common framework mappings

APEC CBPR System | CCPA/CPRA | UK DPA 2018 | GDPR | ISO 27001:2022 | ISO 27701 | ISO 29100 | NIST Privacy Framework v1.0

Official resources

UK GDPR text on legislation.gov.uk

Regulation (EU) 2016/679 as it forms part of UK law, with the Data (Use and Access) Act 2025 amendments, article by article.

legislation.gov.uk/eur/2016/679/contents

ICO: UK GDPR guidance and resources

The regulator's guidance hub for the UK GDPR, by topic: lawful basis, rights, security, breaches and transfers.

ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources

ICO Data Protection Impact Assessments

Outlines how to conduct data protection impact assessments under UK GDPR.

ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias

ICO data protection audit framework

The ICO's audit framework toolkits for checking accountability and governance against the UK GDPR.

ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework

Frequently asked questions

What are the maximum fines under the UK GDPR?

Article 83(5) allows up to 17.5 million pounds or, for an undertaking, 4 percent of total worldwide annual turnover in the preceding financial year, whichever is higher, for infringements of the Article 5 principles, the Article 6, 7 and 9 conditions, data subject rights, the Article 22B and 22C restrictions and the transfer rules. Article 83(4) sets up to 8.7 million pounds or 2 percent for breaches of obligations such as Articles 8, 11 and 25 to 39. The Information Commission issues penalties under sections 155 to 157 of the Data Protection Act 2018.

What is a recognized legitimate interest?

It is a lawful basis in Article 6(1)(ea), in force since February 5, 2026, for processing necessary for a purpose listed in Annex 1: disclosures to a body that needs the data for a public task, national security, public security and defense, emergencies, crime, and safeguarding vulnerable individuals. It is separate from the legitimate interests basis in Article 6(1)(f), and neither applies to public authorities performing their tasks. A significant automated decision cannot rely on it (Article 22B(4)).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How long does a controller have to answer a data subject request?

The applicable time period is one month beginning with the latest of receipt of the request, receipt of information requested to confirm identity and payment of any fee (Article 12A). The controller can extend by two further months by notice within the first month, giving reasons, where requests are complex or numerous. If it needs more information to locate the data under Article 15, the time spent waiting does not count. Subject access need only cover a reasonable and proportionate search (Article 15(1A)).

When must a personal data breach be reported?

Article 33 requires the controller to notify the Information Commission without undue delay and, where feasible, within 72 hours of becoming aware of a breach, unless it is unlikely to result in a risk to people's rights and freedoms. A late notice must give reasons for the delay. A processor must tell the controller without undue delay. Article 34 separately requires communication to individuals where the breach is likely to result in a high risk.

Who must appoint a UK representative?

Under Article 27, a controller or processor outside the UK that is caught by Article 3(2) because it offers goods or services to people in the UK or monitors their behavior there must designate in writing a representative in the UK. The duty does not apply to occasional processing that is unlikely to risk people's rights and does not involve large-scale special category or criminal offence data, nor to public authorities. The representative can be addressed by the Commission and data subjects on all compliance matters.

License included / downloadable: Yes The UK GDPR is UK legislation published free on legislation.gov.uk; the platform links to the official text.

Full framework page and mappings: smartsuite.com/frameworks/uk-gdpr-united-kingdom-general-data-protection-regulation