SmartSuite

Framework / Privacy / Other

Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD/LEGAL/0188, 1980, revised 2013)

The OECD Privacy Guidelines (OECD/LEGAL/0188, 1980, revised 2013) set the eight basic privacy principles, the privacy management program and the transborder flow rules behind privacy laws.



What it is

The OECD Privacy Guidelines are the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, the Annex to an OECD Council Recommendation (OECD/LEGAL/0188) adopted on September 23, 1980 and revised on July 11, 2013; they are the first internationally agreed set of privacy principles and the OECD describes them as the global minimum standard for privacy and data protection. The Recommendation is addressed to Adherents, the 38 OECD member countries and any non-member invited to adhere, and is not legally binding: OECD Recommendations represent a political commitment and an expectation that Adherents will do their best to implement them.

The Guidelines apply to personal data in the public and private sectors which, because of the manner in which they are processed, their nature or the context of their use, pose a risk to privacy and individual liberties (paragraph 2). Part Two sets out the eight Basic Principles of National Application: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability (paragraphs 7 to 14). The 2013 revision kept those principles and added Part Three, Implementing Accountability, which asks every data controller to operate a privacy management program and to notify significant security breaches (paragraph 15).

At a glance

PUBLISHER Organisation for Economic Co-operation and Development (OECD)	TYPE Guidance	VERSION OECD/LEGAL/0188 (1980, revised July 11, 2013)
EFFECTIVE July 11, 2013	DOMAIN Privacy	FAMILY Other
REGION International	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Why it matters

- **One set of principles behind many laws** The eight Basic Principles of National Application (paragraphs 7 to 14) give a privacy program a structure that reads across jurisdictions, because the laws of the Adherents build on them.
- **A defined privacy management program** Paragraph 15 lists what a data controller's program must do, from giving effect to the Guidelines for all personal data under its control to being updated through monitoring and periodic assessment.
- **Risk-based safeguards** The 2013 revision grounded implementation in risk management: safeguards are to be based on privacy risk assessment, and restrictions on transborder flows proportionate to the risks presented (paragraphs 15 and 18).
- **Breach notification expectation** Paragraph 15(c) asks data controllers to notify privacy enforcement authorities of a significant security breach affecting personal data and to notify data subjects where the breach is likely to adversely affect them.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports OECD Privacy Guidelines

Privacy Management Program Record

Document the program paragraph 15(a) describes, tailored to the structure, scale, volume and sensitivity of operations, integrated into governance with internal oversight, and updated through monitoring and periodic assessment, so it can be demonstrated to a privacy enforcement authority on request.

Data Inventory by Purpose

Use Privacy Management to keep an inventory of personal data with the purposes specified at collection, the lawful and fair means of collection and the permitted uses, giving effect to paragraphs 7, 9 and 10.

Privacy Risk Assessments

Record the privacy risk assessments on which paragraph 15(a)(iii) says safeguards should be based, link each risk to the security safeguards of paragraph 11 and track the resulting actions to closure.

Individual Participation Requests

Log requests for confirmation, access, reasons for denial and correction under paragraph 13, with due dates, the form of response and the outcome, including erasure, rectification, completion or amendment.

Breach Notice Log

Record significant security breaches affecting personal data, the assessment of likely adverse effect on data subjects, and the notices given to authorities and individuals under paragraph 15(c), with dates and evidence.

Transborder Flow Safeguards

Use Third Party Risk Management to hold the recipients of transborder flows and the safeguards and enforcement mechanisms that keep protection consistent with the Guidelines (paragraph 17), with the controller's accountability under paragraph 16 assigned to a named owner.

Common framework mappings

APEC CBPR System · APEC PF · Convention 108+ · GDPR · ISO 27001:2022 · ISO 27701 · ISO 29100 · NIST Privacy Framework v1.0

Official resources

OECD Privacy Guidelines

Provides foundational principles for personal data protection and cross-border data flows.

oecd.org/sti/ieconomy/privacy.htm

OECD Guidelines Overview

Describes the structure and scope of the OECD Privacy Guidelines.

oecd.org/internet/ieconomy/guidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Frequently asked questions

What are the eight principles of the OECD Privacy Guidelines?

Part Two sets out the Basic Principles of National Application: collection limitation (paragraph 7), data quality (8), purpose specification (9), use limitation (10), security safeguards (11), openness (12), individual participation (13) and accountability (14). Paragraph 3 says the principles are complementary and should be read as a whole, and the OECD reports that the 2013 revision and the 2021 implementation report both reaffirmed their validity.

Are the OECD Privacy Guidelines legally binding?

No. They are the Annex to a Recommendation of the OECD Council, and OECD Recommendations are not legally binding; they represent a political commitment to the principles they contain and an expectation that Adherents will do their best to implement them. Paragraph 6 treats the Guidelines as minimum standards, and Part Five asks Adherents to adopt laws protecting privacy and to establish privacy enforcement authorities, which is where enforceable obligations arise.

What did the 2013 revision change?

The Council revised the 1980 Recommendation on July 11, 2013 after concluding that the core principles did not need rethinking. The revision focused on practical implementation grounded in risk management and on the global dimension of privacy, introduced national privacy strategies, privacy management programs and data security breach notification, and added Part Three, Implementing Accountability. A supplementary Explanatory Memorandum was produced to support the revised parts, alongside the 1980 Explanatory Memorandum.

What does a privacy management program have to include under Part Three?

Paragraph 15(a) says a data controller's program should give effect to the Guidelines for all personal data under its control, be tailored to the structure, scale, volume and sensitivity of its operations, provide appropriate safeguards based on privacy risk assessment, be integrated into its governance structure with internal oversight mechanisms, include plans for responding to inquiries and incidents, and be updated in light of ongoing monitoring and periodic assessment. Paragraph 15(b) asks the controller to be prepared to demonstrate the program, in particular at the request of a privacy enforcement authority, and 15(c) asks for notice of significant security breaches.

What do the Guidelines say about transborder data flows?

Part Four states that a data controller remains accountable for personal data under its control without regard to the location of the data (paragraph 16), that a member country should refrain from restricting flows to a country that substantially observes the Guidelines or where sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures by the data controller (paragraph 17), and that any restriction should be proportionate to the risks presented, taking into account the sensitivity of the data and the purpose and context of the processing (paragraph 18). The 2021 report found over 84 percent of responding Adherents party to at least one multilateral agreement on legitimate restrictions to such flows.

License included / downloadable: Yes OECD/LEGAL/0188 is published free of charge in the Compendium of OECD Legal Instruments and may be reproduced and distributed without alteration; the English and French texts are the only official versions.

Full framework page and mappings: smartsuite.com/frameworks/oecd-privacy-guidelines