INTERNATIONAL STANDARD

ISO/IEC 27559

First edition
2022-11

Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework

Sécurité de l'information, cybersécurité et protection de la vie privée — Cadre pour la dé-identification de données pour la protection de la vie privée

Reference number
ISO/IEC 27559:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 27, *Information security, cybersecurity and privacy protection.*

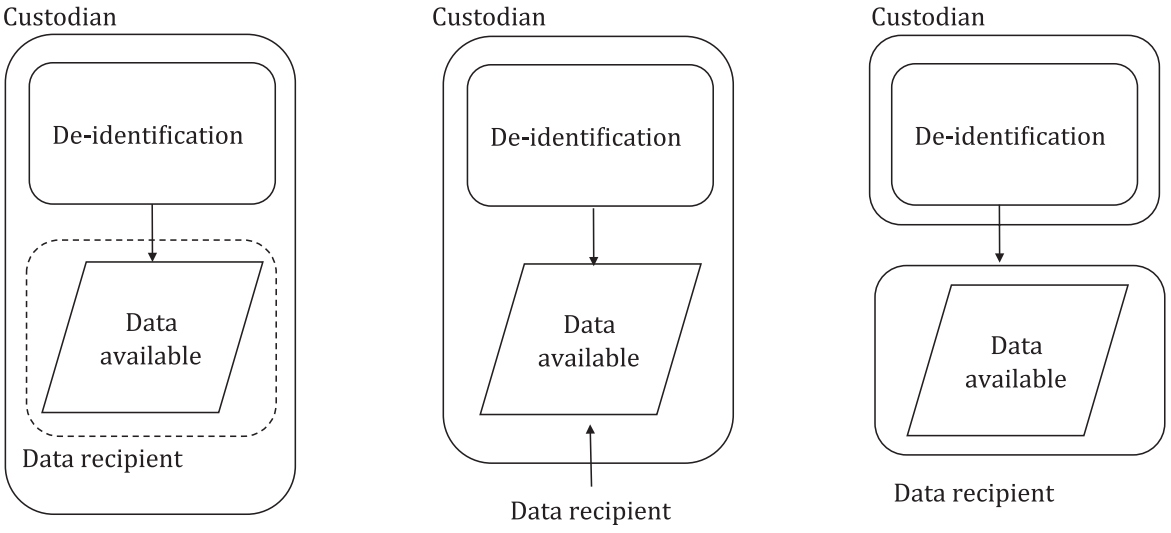
Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

De-identification is one potential means for facilitating the use of personally identifiable information (PII) in a way that does not identify or otherwise compromise the privacy of an individual or a group of individuals. The appropriate use of de-identification techniques can support compliance with regulatory requirements and relevant privacy principles. However, the term "data principal" used in this document is broader than "PII principal" and, for example, includes organizations and computers.

In almost all cases de-identification requires, at the very least, an evaluation of the additional information available to an individual or group that can inappropriately reveal or uncover PII (which is referred to as an adversary, whether a data principal is identified intentionally or not), and how they can combine it to reveal or uncover PII. In short, de-identification requires an assessment of the environment and the circumstances in which the data are made available to data recipients. This considers what additional information is available to an adversary and the possibility of attacks and motivation to re-identify. De-identification also requires an assessment of the data. This determines how the additional information available to an adversary can be used to reveal or uncover PII and the possibility of re-identification, or identity disclosure, by itself or attacks of inference.

This document provides organizations with an implementation framework to govern the appropriate use of data de-identification techniques described in ISO/IEC 20889. This de-identification framework can be applied at any point in the data lifecycle: from designing the means of data collection, the internal reuse of that data, making data available to external partners, or archival. The data recipients can therefore be internal or external to the data custodian that is implementing procedures and practices in accordance with this de-identification framework. As shown in Figure 1 a), use and reuse implies the custodian maintains oversight over the de-identified data while making it available to an internal department or functional group. Figure 1 b) shows external sharing, which implies the custodian maintains oversight over the de-identified data while making it available to an external data recipient (e.g. through a virtual access portal, or a physical data centre). Figure 1 c) shows external release, which implies the custodian transfers oversight over the de-identified data to an external data recipient. In each of these cases, the process of de-identification itself can be transferred to a third party, separate from the custodian or recipient. Written agreements with the recipient determine how data made available after de-identification can be used, in accordance with applicable laws.



a) Use and reuse **b) External sharing** **c) External release**

Figure 1 — Data availability

Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework

1 Scope

This document provides a framework for identifying and mitigating re-identification risks and risks associated with the lifecycle of de-identified data.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, that are PII controllers or PII processors acting on a controller's behalf, implementing data de-identification processes for privacy enhancing purposes.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*

ISO 31000, *Risk Management — Guidelines*