

---

---

**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*





**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>v</b>
<b>Introduction</b>	<b>vi</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>1</b>
<b>4 Symbols and abbreviated terms</b>	<b>3</b>
<b>5 Overview</b>	<b>3</b>
<b>6 Context assessment</b>	<b>4</b>
6.1 General	4
6.2 Threat modelling	4
6.2.1 General	4
6.2.2 Security and privacy practices	5
6.2.3 Motives and capacity to re-identify	5
6.3 Transparency and impact assessment	6
6.3.1 General	6
6.3.2 Transparency of actions and stakeholder engagement	6
6.3.3 Privacy-related harms	6
<b>7 Data assessment</b>	<b>7</b>
7.1 General	7
7.2 Data features	7
7.2.1 General	7
7.2.2 Data principals	7
7.2.3 Data type	7
7.2.4 Attribute types	8
7.2.5 Dataset properties	8
7.3 Attack modelling	8
7.3.1 General	8
7.3.2 Maximum or average risk	9
7.3.3 Population or sample-based attack	9
7.3.4 Data privacy models	9
<b>8 Identifiability assessment and mitigation</b>	<b>10</b>
8.1 General	10
8.2 Assessing identifiability	10
8.2.1 General	10
8.2.2 Quantifying identifiability	10
8.2.3 Adversarial testing	11
8.3 Mitigation	12
8.3.1 General	12
8.3.2 Reconfiguring the environment	12
8.3.3 Transforming the data	12
8.3.4 Re-evaluation	13
<b>9 De-identification governance</b>	<b>13</b>
9.1 General	13
9.2 Before data are made available	13
9.2.1 General	13
9.2.2 Assigning roles and responsibilities	13
9.2.3 Establishing principles, policies and procedures	14
9.2.4 Identifying and managing a data disclosure	14
9.2.5 Communicating with stakeholders	15
9.3 After data are made available	15
9.3.1 General	15

9.3.2 Monitoring the data environment ..... 15

9.4 Mitigation in case of incident..... 15

**Annex A (informative) Example identifiers ..... 17**

**Annex B (informative) Example threshold identifiability benchmarks..... 19**

**Bibliography ..... 21**

## 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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://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](http://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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://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.

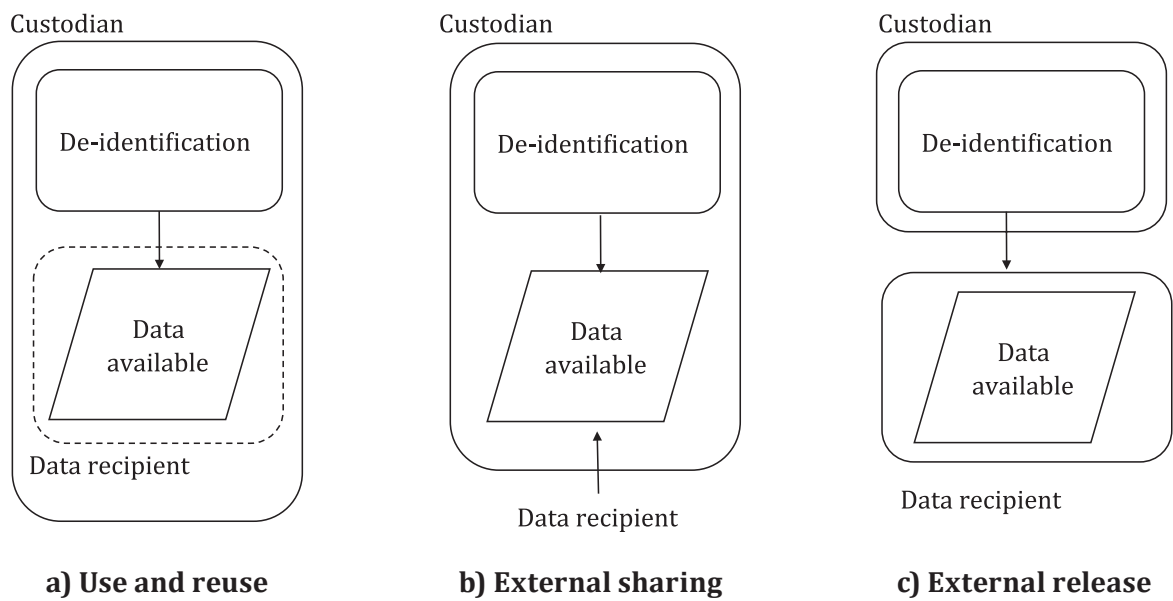


Figure 1 — Data availability

# 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*