



Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN ISO/IEC 29134:2020

Information technology - Security techniques - Guidelines for privacy impact assessment (ISO/IEC 29134:2017)

Informationstechnik -
Sicherheitsverfahren - Leitlinien für die
Datenschutz-Folgenabschätzung (ISO/
IEC 29134:2017)

Technologies de l'information -
Techniques de sécurité - Lignes
directrices pour l'évaluation d'impacts
sur la vie privée (ISO/IEC 29134:2017)

03/2020



National Foreword

This European Standard EN ISO/IEC 29134:2020 was adopted as Luxembourgish Standard ILNAS-EN ISO/IEC 29134:2020.

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

THIS PUBLICATION IS COPYRIGHT PROTECTED

Nothing from this publication may be reproduced or utilized in any form or by any mean - electronic, mechanical, photocopying or any other data carries without prior permission!

English version

Information technology - Security techniques - Guidelines for privacy impact assessment (ISO/IEC 29134:2017)

Technologies de l'information - Techniques de sécurité
- Lignes directrices pour l'évaluation d'impacts sur la
vie privée (ISO/IEC 29134:2017)

Informationstechnik - Sicherheitsverfahren -
Datenschutz-Folgenabschätzung - Leitfaden (ISO/IEC
29134:2017)

This European Standard was approved by CEN on 2 March 2020.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Contents	Page
European foreword.....	3

European foreword

The text of ISO/IEC 29134:2017 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 29134:2020 by Technical Committee CEN/CLC/JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2020, and conflicting national standards shall be withdrawn at the latest by September 2020.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 29134:2017 has been approved by CEN as EN ISO/IEC 29134:2020 without any modification.

First edition
2017-06

Information technology — Security techniques — Guidelines for privacy impact assessment

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'évaluation d'impacts sur la vie privée

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	3
5 Preparing the grounds for PIA	4
5.1 Benefits of carrying out a PIA	4
5.2 Objectives of PIA reporting	5
5.3 Accountability to conduct a PIA	5
5.4 Scale of a PIA	6
6 Guidance on the process for conducting a PIA	6
6.1 General	6
6.2 Determine whether a PIA is necessary (threshold analysis)	7
6.3 Preparation of the PIA	7
6.3.1 Set up the PIA team and provide it with direction	7
6.3.2 Prepare a PIA plan and determine the necessary resources for conducting the PIA	9
6.3.3 Describe what is being assessed	10
6.3.4 Stakeholder engagement	11
6.4 Perform the PIA	13
6.4.1 Identify information flows of PII	13
6.4.2 Analyse the implications of the use case	14
6.4.3 Determine the relevant privacy safeguarding requirements	15
6.4.4 Assess privacy risk	16
6.4.5 Prepare for treating privacy risks	19
6.5 Follow up the PIA	23
6.5.1 Prepare the report	23
6.5.2 Publication	24
6.5.3 Implement privacy risk treatment plans	24
6.5.4 Review and/or audit of the PIA	25
6.5.5 Reflect changes to the process	26
7 PIA report	26
7.1 General	26
7.2 Report structure	27
7.3 Scope of PIA	27
7.3.1 Process under evaluation	27
7.3.2 Risk criteria	29
7.3.3 Resources and people involved	29
7.3.4 Stakeholder consultation	29
7.4 Privacy requirements	29
7.5 Risk assessment	29
7.5.1 Risk sources	29
7.5.2 Threats and their likelihood	29
7.5.3 Consequences and their level of impact	30
7.5.4 Risk evaluation	30
7.5.5 Compliance analysis	30
7.6 Risk treatment plan	30
7.7 Conclusion and decisions	30
7.8 PIA public summary	30
Annex A (informative) Scale criteria on the level of impact and on the likelihood	32