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

*Information technology — Security techniques — Guidelines for
privacy impact assessment*



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2017

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos.....	v
Introduction.....	vi
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Abréviations	3
5 Préparation de la justification d'un PIA	4
5.1 Avantages de la mise en œuvre d'un PIA.....	4
5.2 Objectifs de la production de rapports de PIA.....	5
5.3 Responsabilité de la conduite d'un PIA.....	6
5.4 Échelle d'un PIA.....	6
6 Recommandations relatives au processus de conduite d'un PIA	7
6.1 Généralités.....	7
6.2 Déterminer si un PIA est nécessaire (analyse du seuil).....	7
6.3 Préparation du PIA.....	8
6.3.1 Constituer l'équipe de PIA et lui donner des directives.....	8
6.3.2 Préparer un plan de PIA et déterminer les ressources nécessaires à la conduite du PIA.....	10
6.3.3 Décrire ce qui est évalué.....	11
6.3.4 Engagement des parties prenantes.....	12
6.4 Exécuter le PIA.....	15
6.4.1 Identifier les flux d'informations des DCP.....	15
6.4.2 Analyser les implications du cas d'utilisation.....	16
6.4.3 Déterminer les exigences applicables en matière de protection de la vie privée.....	16
6.4.4 Évaluer le risque sur la vie privée.....	17
6.4.5 Préparer le traitement des risques sur la vie privée.....	21
6.5 Assurer le suivi du PIA.....	26
6.5.1 Préparer le rapport.....	26
6.5.2 Publication.....	26
6.5.3 Mettre en œuvre les plans de traitement des risques sur la vie privée.....	27
6.5.4 Examen et/ou audit du PIA.....	28
6.5.5 Refléter les changements de processus.....	28
7 Rapport de PIA	29
7.1 Généralités.....	29
7.2 Structure de rapport.....	29
7.3 Domaine d'application du PIA.....	30
7.3.1 Processus soumis à évaluation.....	30
7.3.2 Critères de risque.....	32
7.3.3 Ressources et personnes impliquées.....	32
7.3.4 Consultation des parties prenantes.....	32
7.4 Exigences relatives à la protection de la vie privée.....	32
7.5 Évaluation des risques.....	32
7.5.1 Sources de risque.....	32
7.5.2 Menaces et probabilité associée.....	33
7.5.3 Conséquences et niveau d'impact associé.....	33
7.5.4 Évaluation des risques.....	33
7.5.5 Analyse de conformité.....	33
7.6 Plan de traitement des risques.....	33
7.7 Conclusion et décisions.....	33
7.8 Résumé public du PIA.....	33
Annexe A (informative) Critères d'échelle sur le niveau d'impact et la probabilité	35