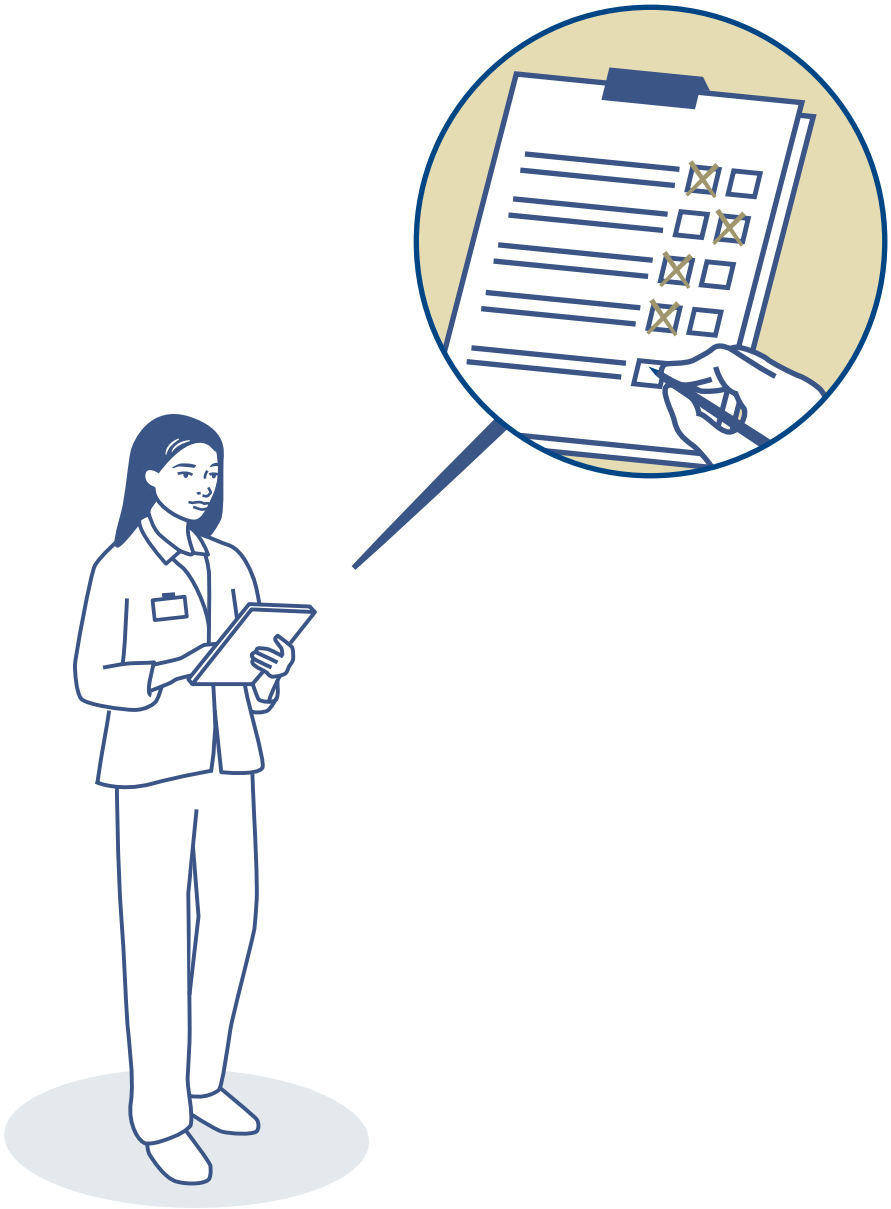
Guide pour le registre des activités de traitement



Version du 03/2023

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

Préambule

La nouvelle loi fédérale sur la protection des données (LPD) et son ordonnance (OPDo) ont pour but de protéger la personnalité et les droits fondamentaux des personnes physiques. Pour atteindre ce but, la loi et l'ordonnance définissent des exigences concernant le traitement des données personnelles.

Les cabinets médicaux et les médecins ainsi que leurs auxiliaires traitent de nombreuses données personnelles dans le cadre de leur activité. Ils doivent donc entre autres respecter et appliquer les prescriptions de la LPD.

Le présent document et d'autres documents mis à disposition visent à faciliter l'application et le respect des prescriptions en matière de protection des données.

Table des matières

1 Définitions

Terme	Description
Données personnelles / données sensibles	Sont considérées comme **données personnelles** toutes les informations concernant une personne identifiée ou identifiable. La question de savoir si une personne est directement ou indirectement déterminable ou identifiable dépend notamment du contexte dans lequel les données se trouvent ou sont traitées. Les données personnelles sont notamment les informations personnelles, les coordonnées, le sexe, la date de naissance, l'activité professionnelle, etc. Selon la LPD, les **données sensibles** comprennent les données qui renseignent sur : — la santé (p. ex. l'état de santé, les diagnostics, les traitements, etc.) et la sphère intime (p. ex. la sexualité) ; — l'origine raciale ou ethnique, — les opinions ou les activités religieuses, philosophiques, politiques ou syndicales ; — les mesures d'aide sociale ; et — les poursuites ou sanctions pénales ou administratives. Les données génétiques et les données biométriques qui permettent d'identifier une personne de manière univoque font également partie des données sensibles.
Profilage	On entend par **profilage** toute forme de traitement automatisé de données personnelles visant à évaluer, analyser ou prédire les aspects personnels d'une personne physique. Conformément à la LPD, les aspects personnels suivants en particulier sont utilisés pour analyser ou prédire : « le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements ».
Supports de données	La définition de **support de données** s'applique pour l'utilisation de supports de données tant physiques que numériques.
Supports de données numériques (amovibles)	Sont notamment considérés comme **supports de données numériques (amovibles)** les CD / DVD, les clés USB, les disques durs externes, les bandes magnétiques, les ordinateurs portables, les serveurs, etc.
Supports de données physiques	Les documents papier sont par exemple des **supports de données physiques**.
Traitement	Le **traitement** des données comprend toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés. Par traitement, on entend donc notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement et la destruction de données personnelles.
Traitement automatisé	On entend par **traitement automatisé** le traitement (cf. la notion de « traitement ») de données personnelles au moyen de procédés automatisés. Un traitement est **automatisé** lorsqu'il est effectué sous une forme structurée, généralement au moyen d'installations de traitement de données (p. ex. serveurs, services de communication, ordinateurs, systèmes ou programmes informatiques). Ne sont pas considérés comme des traitements automatisés les stockages de données analogues, tels que les archives papier non structurées ou les traces écrites.

2 Guide relatif au modèle de registre des activités de traitement

2.1 Généralités

Avec l'entrée en vigueur de la nouvelle loi fédérale sur la protection des données (LPD), les responsables du traitement ont l'obligation, à certaines conditions, de tenir un registre des activités de traitement. Cette obligation concerne les responsables qui emploient plus de 250 collaboratrices et collaborateurs ainsi que les responsables qui procèdent à un traitement à grande échelle de données sensibles. En raison de la sensibilité des données sur la santé, il est recommandé aux médecins et aux cabinets d'inscrire dans le registre des activités de traitement au moins celles qui sont centrées sur le traitement de données sensibles (p. ex. tenue et gestion des dossiers médicaux, gestion des données de la patientèle relatives au décompte des assurances sociales, gestion du personnel, etc.). En principe, tant la personne responsable du traitement (comme le cabinet médical) que certains sous-traitants (comme le centre de décompte) doivent chacun tenir un registre.

2.2 Instructions pour remplir le registre

Les explications suivantes relatives aux différentes colonnes du registre sont destinées à aider les responsables à remplir le modèle. Les colonnes indiquées correspondent aux indications légales minimales qui doivent figurer dans le registre. Le modèle contient quelques exemples (marqués en rouge) qui peuvent être adaptés, complétés ou supprimés lorsque les activités de traitement proposées ne sont pas pertinentes.

Activité de traitement	Indiquer ici l'activité de traitement spécifique lors de laquelle des données personnelles sont traitées. Lorsque cela s'avère judicieux, des activités de traitement connexes ou similaires peuvent aussi être regroupées en une seule activité de traitement. La désignation de l'activité devrait être aussi claire que possible et indiquer comment et dans quel contexte les données personnelles sont traitées.
Finalité	La finalité du traitement des données personnelles doit être indiquée dans cette colonne. Il est aussi possible de mentionner plusieurs finalités.
Responsables	Indiquer ici la personne responsable de l'activité de traitement et des données traitées. La personne responsable est celle qui décide comment et avec quoi les données sont traitées (p. ex. la ou le médecin). Lorsque plusieurs personnes sont responsables d'une activité de traitement (p. ex. la tenue des dossiers médicaux dans un cabinet de groupe), il est recommandé d'indiquer le nom du cabinet médical ainsi que les fonctions des responsables (p. ex. médecin traitant). Il existe notamment plusieurs responsables du traitement lorsque plusieurs personnes décident des procédures et moyens utilisés pour le traitement (p. ex. la direction).
Catégories de personnes concernées	Il s'agit d'indiquer les catégories de personnes concernées dont les données sont traitées. Par catégories de personnes concernées, on entend des groupes présentant certaines caractéristiques communes (p. ex. personnes intéressées, patientèle, personnel, prestataires de services, etc.).
Catégories de données personnelles	Ici, les données personnelles traitées peuvent être regroupées en catégories (p. ex. informations personnelles, données de base, coordonnées, données salariales, données d'assurance [sociale], coordonnées bancaires, données relatives au traitement médical, données sur la santé, etc.). La catégorisation peut être plus ou moins détaillée.

Catégorie de destinataires	De même, les destinataires qui, dans le cadre d'une activité, ont accès aux données personnelles ou peuvent les consulter peuvent être regroupés en catégories. Peu importe que les données soient activement transférées aux destinataires ou que ceux-ci y aient un accès direct. Les destinataires peuvent être des personnes, des entreprises, des autorités, etc. Il est recommandé de choisir une dénomination claire pour chaque catégorie de destinataires (p. ex. caisses-maladie, assurance-invalidité, comptabilité, administration fiscale, autorités de surveillance, prestataires de services [informatiques], etc.).
Délai de conservation / critère pour déterminer la durée de conservation	S'ils sont connus, il convient d'indiquer les délais concrets de conservation des données (p. ex. nombre de jours ou d'années). Il convient alors de tenir compte en particulier des obligations de conservation légales et déontologiques. En l'absence de délais de conservation légaux ou déontologiques, il convient de préciser selon quels critères les données personnelles sont conservées (p. ex. jusqu'à l'atteinte de la finalité, jusqu'au départ de la collaboratrice ou du collaborateur).
Mesures relatives à la sécurité des données	Il convient de préciser ici, le cas échéant, quelles mesures techniques et organisationnelles sont déjà mises en œuvre afin de protéger les données contre toute perte de confidentialité, d'intégrité et de disponibilité (p. ex. armoires verrouillées pour les dossiers médicaux physiques, trafic d'e-mails chiffrés, restriction d'accès aux archives numériques, formation du personnel, etc.). Il est en principe aussi possible de renvoyer à des concepts de sécurité existants.
Communication à l'étranger	Il convient d'inscrire « oui » ou « non » dans cette colonne pour indiquer si des données personnelles sont communiquées à l'étranger dans le cadre d'une activité de traitement. Il y a communication notamment lorsque les données personnelles sont transmises à un-e autre médecin ou à un laboratoire à l'étranger, ou lorsque l'activité de traitement utilise un système dont le prestataire, qui a son siège à l'étranger, peut ainsi potentiellement accéder aux données (p. ex. recours à de systèmes basés sur le cloud, dès lors que le prestataire a ou pourrait avoir accès aux données en texte clair).
Désignation de l'État et garantie/outil	Si vous avez répondu « oui » à la question relative à la communication de données personnelles à l'étranger, veuillez nommer l'État concerné. Il convient en outre de préciser de quelle manière la protection adéquate des données personnelles et, partant, des droits de la personnalité des personnes concernées est garantie. En raison de la complexité des processus informatiques, il est recommandé de vérifier auprès du prestataire informatique concerné si des données personnelles sont communiquées à l'étranger. Si tel est le cas, il convient en outre de clarifier les mesures prises pour respecter les prescriptions légales. La protection des données est considérée comme garantie lorsque le Conseil fédéral a pris une décision d'adéquation pour le pays ou le gouvernement concerné. La liste des États [1] indique ceux pour lesquels une telle décision d'adéquation a été prise. En l'absence d'une telle législation, la loi soumet la communication à l'étranger à d'autres conditions (art. 16 ss LPD). En l'absence de décision d'adéquation et si la base légale dans le pays destinataire est insuffisante, il est recommandé de renoncer à communiquer des données personnelles à l'étranger, en particulier en présence d'un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Dans tous les cas, il convient de veiller à ce que la protection des données et, en particulier, la sécurité des données, soient garanties. Les données sur la santé sont en outre des données sensibles. Des mesures techniques et organisationnelles appropriées doivent tenir compte du besoin accru de protection. Les exigences minimales en matière de sécurité des données sont réglées dans l'ordonnance sur la protection des données (OPDo). Les exigences minimales pour la sécurité informatique offrent en outre une aide supplémentaire en matière de sécurité des données [2].

[1] Annexe 1 de l'ordonnance sur la protection des données (OPDo)
[2] https://www.fmh.ch/. Prestations / EHealth / Exigences minimales pour la sécurité informatique

Impressum
Edition: FMH – Fédération des médecins suisses, Berne
Publication: mars 2023
www.fmh.ch