Newsletter
#02 / 2017

Chère lectrice, cher lecteur,
Comme tous les organes publics, notre Autorité fait face, dans ses domaines d'activité, à un changement et à de constants nouveaux défis. Nous attachons de l'importance à ce que les bases légales en tiennent compte. S'agissant de la transparence, nous venons d'achever une actualisation correspondante, alors que la révision de la Loi sur la protection des données a commencé en parallèle. Dans les deux cas, nous voulons notamment harmoniser nos bases légales cantonales avec les normes internationales.

L'année dernière, la Loi sur l'information et l'accès aux documents (LInf) a été adaptée à la Convention d'Aarhus, qui engage la Suisse dans le domaine de l'environnement. La révision de l'Ordonnance sur l'accès aux documents (OAD) entre en vigueur le 1er janvier 2018. En sus des modifications indispensables, certaines adaptations de la loi et de l'ordonnance tiennent compte des expériences des sept dernières années dans l'application de la législation sur l'accès aux documents.

En matière de protection des données, des modifications importantes de la législation nous attendent. Le 15 septembre 2017, le Conseil fédéral a publié l'avant-projet et le message relatifs à la révision totale de la Loi fédérale sur la protection des données. Celle-ci doit tenir compte de la révision de la législation européenne pour que la Suisse continue de disposer d'un bon niveau de protection des données. C'est d'une importance capitale pour l'économie afin que l'échange de données avec l'UE ne soit pas excessivement difficile.

A l'échelle cantonale, nous devons aussi examiner si et dans quelle mesure il y a lieu d'adapter la Loi sur la protection des données. Il s'agit notamment de prendre en compte l'actualisation de la Convention STE 108 du Conseil de l'Europe et la Directive (UE) 2016/680. Cette dernière fait partie de l'acquis de Schengen. Si les autorités suisses, en particulier dans les domaines de la police et du droit pénal, souhaitent avoir accès au Système d'information Schengen (SIS), il est aussi nécessaire de réviser la législation cantonale.

En plus de ces adaptations légales, il y a encore de nombreux autres sujets d'actualité dans nos domaines d'activité, dont certains sont abordés dans la présente newsletter. Nous vous souhaitons une agréable lecture !

Alice Reichmuth Pfammatter
Préposée cantonale à la protection des données

Annette Zunzer Raemy
Préposée cantonale à la transparence

ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

EC 902

Sommaire

Editorial 1

Actualités 2
Développement continu de l'Open Data en Suisse 2
Cookies et traçabilité 3
Analyse des pratiques de Facebook 4
Voitures connectées et traitement des données 4
Nouveauté dans le droit de la santé 5
Dossier électronique du patient et protection des données 5
Vidéosurveillance sur le lieu de travail 6
Des données sensibles sur la santé pour tous? 7

Informations aux organes publics 8
Externalisation – Cloud 8
Adaptation de l'ordonnance sur l'accès aux documents 8
Etude sur un identifiant personnel unique 9

Actualités

Développement continu de l'Open Data en Suisse

La conférence annuelle 2017 d'Opendata.ch était consacrée à l'avenir des données ouvertes en Suisse. Les données ouvertes, de même que les infrastructures de données, sont aujourd'hui exploitées par quasi tout le monde, dans tous les aspects de la vie ou presque, qu'il s'agisse des sciences, du secteur alimentaire, du développement urbain, du tourisme ou des transports.

Lors de la conférence, les représentantes et les représentants de la société numérique ont présenté ces domaines et discuté avec les participants issus des secteurs de l'administration, de l'économie, des sciences, de la politique, du journalisme et de l'informatique au sujet de programmes de développement visant à obtenir plus d'efficacité, de transparence et d'innovation à l'aide des données publiques, de même qu'à créer un environnement progressiste en matière écologique, technologique et sociale.

Atouts de la Suisse

Ainsi, Peter Delfosse, CEO de l'entreprise Axon Active, qui offre des services de numérisation, plaide pour une interprétation à long terme des données et leur regroupement au sein d'écosystèmes. Les données ne sont pas des biens de consommation, selon ce dernier, mais des biens d'investissement. Et la Suisse possède des atouts dans ce processus, c'est-à-dire des conditions de réalisation propices et une force d'innovation qu'il convient d'exploiter. Par ailleurs, Peter Delfosse estime qu'il est indispensable que l'Open Data soit reconnue au plus haut niveau de direction, que l'administration soit habilitée à procéder à la transformation numérique et que la population ainsi que les parlements soient impliqués.

Selon Simon Hodson, directeur de CODATA, le Comité de données pour la science et la technologie, il est impératif d'investir dans l'infrastructure de données de la même façon que l'on investissait autrefois dans les bibliothèques. En outre, il juge indispensable que les données ayant servi à mener des études scientifiques soient rendues publiques parallèlement à celles-ci. À défaut de cela, la science ne serait pas transparente.

Lors de la conférence, Rahel Ryf, de la plateforme Open Data des TP suisses, a montré comment concevoir le futur numérique des transports publics à l'aide de l'Open Data et Pascal Jenny, directeur touristique à Arosa, a exposé le potentiel des données publiques pour le tourisme en montagne suisse.

Multiplicité des usages

Andreas Kellerhals, directeur des Archives fédérales suisses, a pour sa part donné un aperçu de l'état actuel ainsi que des perspectives et objectifs poursuivis par opendata.swiss, le portail des données ouvertes de l'administration publique suisse. Il constate une augmentation des données de près de 90% par rapport à l'année dernière et une augmentation conséquente de l'utilisation des données sur le portail. La stratégie actuelle arrivant à échéance l'année prochaine, il appelle à définir désormais celle qui sera mise en place dès 2019.

La vue d'ensemble des plus de 30 applications créées sur la base des données issues d'opendata.swiss montre bien la diversité des usages que l'on peut en faire. Par exemple, il est possible de rechercher les montagnes des Alpes suisses, de même que l'origine de leurs noms, ou de naviguer dans des paysages photographiés autrefois, à l'aide d'une machine à remonter le temps d'une manière participative. Un assistant de voyage peut répondre à des questions concernant des horaires dans le cadre d'une conversation simple, tandis que d'autres applications permettent de localiser et de se rendre rapidement aux toilettes publiques les plus proches de la ville de Zurich ou de se renseigner en temps réel sur les places disponibles dans les parkings couverts ou les vélos de location disponibles.

Cookies et traçabilité

—

«Autorisez-vous les cookies?». Cette question nous est régulièrement posée lorsque nous visitons des sites Internet. Comment fonctionnent les cookies ?

Les cookies se définissent comme des fichiers qui sont sauvegardés sur le disque dur de l'utilisateur d'un site web après sa première visite (Steiger Martin, Rechtskonforme Cookies auf Websites nach europäischem und schweizerischem Recht, in Anwaltsrevue 2015 p. 18-21). Ils fonctionnent comme une carte de visite qui est propre à chacun. De cette manière, le site se souvient de l'utilisateur et, dans une certaine mesure, de son comportement sur le site. C'est le cas des noms d'utilisateurs, des pages visitées, du nombre de click, des scrolls.

Les cookies laissent des traces. Si celles-ci sont reliées à d'autres informations, elles peuvent former des profils de personnalité et ainsi identifier des personnes. C'est une utilisation possible des services de webtracking.

Cependant, tous les cookies ne sont pas nuisibles. Certains sont même utiles car ils permettent de surfer d'une page à l'autre sans perdre des informations. C'est de cette manière que le e-commerce est possible. Les informations stockées permettent de savoir quelles informations sont mises dans le panier d'achat, par exemple. La gestion des informations dans les boîtes mails se fait à l'aide de cookies également.

Le projet de la nouvelle Directive européenne sur les cookies (ancienne Directive 2009/136/CE) prévoit de simplifier les règles sur l'utilisation des cookies. En soi, l'utilisateur pourra bloquer les cookies directement dans ses paramètres de navigation, mais aucune autorisation ne sera demandée pour les cookies nécessaires à la navigation sur les sites et non intrusifs, ainsi que pour les cookies comptant le nombre de personnes ayant visitées le site. La pratique suisse actuelle, moins restrictive, est réglée par les articles 45c et 53 de la Loi du 30 avril 1997 sur les télécommunications (RS 784.10; LTC). L'obligation est celle d'informer l'usager sur l'existence des cookies et sur les raisons de leur utilisation. Il peut refuser ce traitement par un «opt out».

Analyse des pratiques de Facebook

Lors de la dixième journée suisse du droit de la protection des données qui a eu lieu à Fribourg, un atelier a porté sur le traitement des données effectué par les réseaux sociaux, en particulier quelques pratiques de Facebook ont été analysées.

Après avoir défini les acteurs, le droit applicable et les données personnelles sensibles et non sensibles, le profil de personnalité et le traitement des données, la Loi fédérale sur la protection des données (LPD) a été introduite dans la mesure où Facebook est une personne privée. Pour qu'un réseau social puisse traiter des données personnelles, il faut des motifs justificatifs. Facebook s'appuie à cet effet sur le lien contractuel avec l'utilisateur, à savoir les conditions générales d'utilisation (CGU; par exemple pour la création du compte, la gestion des amis, etc.). Pour le reste, il se fonde sur le consentement de l'utilisateur, partant du principe que la personne qui a un profil consent à tout traitement de données effectué par Facebook. Or, il ressort clairement de l'analyse que Facebook a une position dominante et l'utilisateur a peu de liberté. En effet, soit il accepte tout soit il ne l'utilise pas.

En parcourant les CGU, on s'aperçoit notamment que ces dernières sont vagues, que les traitements sont illimités, que les données sont utilisées pour la recherche scientifique et partagées avec d'autres applications. En outre, la plupart du temps, elles ne sont pas lues par les utilisateurs, en particulier au vu de leur complexité, technicité et exhaustivité. Ainsi, malgré la modification des paramètres, Facebook se permet de traiter énormément de nos données avec notre «pseudo-consentement» puisque l'utilisateur n'est pas clairement informé de tous les traitements effectués avec ses données. Pour conclure, on s'aperçoit qu'il y a un besoin accru de transparence des réseaux sociaux et qu'il est important d'avoir une réglementation stricte et souple mais surtout des moyens juridiques et techniques de l'appliquer et la faire respecter à l'échelon international. N'oublions pas qu'avec l'intelligence artificielle (reconnaissance vocale, faciale), Facebook collecte toujours plus de données et est en mesure de faire des profils de personnalité.

Voitures connectées et traitement des données

Lorsque l'on utilise la navigation ou que l'on écoute de la musique lors d'un trajet en voiture, quelles données sont collectées et traitées par la voiture?

Les véhicules connectés ont accès aux données du détenteur du véhicule mais également à celles de ses passagers. En effet, la voiture peut avoir accès à des données de la personne qui connecte son smartphone (informations des contacts) mais également à des données provenant de l'utilisation du véhicule, à savoir notamment la géolocalisation, la durée du trajet, la position de stationnement, le nombre de resserrement de la ceinture et le nombre de conducteurs différents. Les données collectées ne sont pas seulement accessibles par le garagiste qui fait les contrôles du véhicule mais sont également transmises régulièrement au fournisseur de la marque. Ainsi, on peut déduire de ces informations que selon la marque de la voiture choisie et utilisée, nos données ne sont pas protégées de la même manière.

En effet, les données d'une voiture de marque européenne sont transmises et traitées en Europe, qui a une protection similaire à la Suisse. Par contre, les données collectées par une voiture de marque japonaise ou américaine n'ont pas forcément la même protection étant donné que leur législation n'assure pas un niveau de protection adéquat (cf. liste des Etats sûrs établie par le Préposé fédéral à la protection des données et à la transparence). Ainsi, on réalise que le choix d'un simple véhicule pourra avoir un impact sur l'utilisation de nos propres données. Pour information, voici un lien vous permettant d'avoir un aperçu sur les données collectées et transmises par certaines marques de véhicule à leur fournisseur: https://www.adac.de/infotestrat/adac-im-einsatz/motorwelt/datenkrake_auto.aspx.

Nouveauté dans le droit de la santé

—

La 24e Journée de droit de la santé a abordé les nouveautés du droit général de la santé à l'Université de Neuchâtel.

La législation sur le dossier électronique du patient (DEP) est entrée en vigueur le 15 avril 2017 et constitue sans doute la principale nouveauté dans le domaine du droit de la santé. Le patient est libre de créer ou non un tel dossier. L'utilisation du DEP sera toutefois obligatoire pour les hôpitaux et les cliniques de réadaptation à partir de 2020, à partir de 2022 pour les EMS et les maisons de naissance (cf. résumé sur le DEP). La décision de la Cour européenne des droits de l'homme du 18 octobre 2016 dans l'affaire Vukota-Bojic contre la Suisse a aussi fait des vagues. La cour a établi que la surveillance en secret d'une bénéficiaire de rente par un détective privé contrevient à la CEDH. La base légale d'une telle surveillance fait défaut (https://hudoc.echr.coe.int/eng#{«itemid»:[«001-167490»]}).

Médecine commerciale

Les nouvelles structures d'établissements de santé ont fait l'objet d'une attention particulière. Les cabinets individuels et les petits cabinets sont toujours moins demandés sur le marché. Les grandes structures ont le vent en poupe, que ce soit sous forme de sociétés anonymes ou d'autres structures de droit privé. Selon le médecin cantonal neuchâtelois, le Dr Robert, cette tendance pose de nouveaux défis à l'activité de surveillance en lien avec la mobilité accrue des professionnels de la santé, la libre circulation ou les diplômes délivrés par des institutions de formation étrangères. Par ailleurs, les compétences cantonales fixent des limites à une surveillance intercantonale efficace. Les autorités de surveillance sont de plus en plus sollicitées s'agissant de la défense des droits des patients – à l'instar des droits d'accès, des droits à l'information ou du respect du secret médical. L'exercice de ces droits connaît des difficultés qui vont souvent de pair avec des structures de droit privé exclusivement axées sur les bénéfices et entraînent parfois la fermeture rapide de cabinets.

Le marché de la santé fonctionne-t-il comme n'importe quel autre marché?

Un système de santé publique qui satisfait à des exigences de qualité nécessite une régulation de l'État et de nouvelles bases légales. Il faut des approches appropriées pour garantir une activité de surveillance efficace.

Dossier électronique du patient et protection des données

—

Une Journée d'information de privatim sur le dossier électronique du patient a été organisée, mettant un accent sur le fonctionnement et l'importance de la confiance du/de la patient/e.

Dossier électronique du patient : fonctionnement et risques spécifiques

La protection des données est importante en matière de dossier électronique du patient (ci-après DEP), un grand nombre de données sensibles liées à la santé étant traitées par les patients eux-mêmes, les communautés et communautés de référence, les professionnels de la santé et les prestataires de services informatiques. La législation sur le DEP comporte de nouvelles obligations, auxquelles les participants au DEP doivent se conformer. Le fait justificatif principal permettant le traitement de données dans le DEP est le consentement des patients. Différents types de consentements sont prévus dans l'ordonnance, à savoir sous la forme «opt-in» (la personne concernée doit donner son consentement pour la communication) ou « opt-out » (l'intéressé doit agir pour empêcher la communication). Certaines dispositions prévoyant un consentement de type «opt-out» posent problème du point de vue de la protection des données, car ils conduisent à un accès aux données par les professionnels de la santé bien que ceux-ci n'en aient pas besoin pour remplir leur tâche, ce qui n'est pas conforme au principe de proportionnalité du traitement des données. Le législateur a maintenu cette solution malgré le signalement des groupes de travail de «e-health» Suisse, arguant le fait que l'introduction du consentement «opt-in» pouvait entraver l'introduction du DEP dans la société.

La mise en place de communautés et de communautés de référence au niveau cantonal

La législation prévoit une introduction décentralisée du DEP et définit dans ce but des unités organisationnelles appelées communautés et communautés de référence qui doivent mettre en œuvre les mesures organisationnelles et techniques et auxquelles seuls les professionnels de la santé peuvent participer. En revanche, il n'est pas dit qui assume la responsabilité de les créer et des les exploiter, ni comment les coûts d'exploitation induits par le DEP sont financés. Les cantons se voient attribuer deux

fonctions: ils vérifient les demandes d'aide financière fournies par la Confédération pour la création d'une communauté/communauté de référence en formulant une recommandation et sanctionnent les prestataires de service qui, en violation de la loi, n'adhèrent pas à une communauté. Les cantons sont en outre responsables du système d'approvisionnement de la santé de leur population, dont le DEP promet d'augmenter l'efficience et la qualité, ce qui incite les cantons à s'engager pour l'introduction du DEP. Le canton de Zurich par exemple crée des conditions cadres pour une introduction rapide et généralisée du DEP.

Protection et sécurité des données dans la législation d'application de la LDEP

Seules les données privées d'accès sont absolument sûres, cependant elles sont également inutiles. Il est important, pour que les patients soient traités correctement, de disposer des bonnes informations au bon moment et au bon endroit. Il faut alors trouver un équilibre entre les risques liées à la communication des informations et ceux liés à l'absence de communication. Le DEP étant facultatif, il est important que les patients aient confiance en ce système et, pour cela, une sécurité appropriée est nécessaire, ce qui augmente également les coûts. Trouver un équilibre pour un système complexe tel que l'«e-health» reste un défi pour le législateur qui doit trouver des compromis entre protection et sécurité des données, sécurité des patients, mais également entre les coûts et l'«usability » ainsi qu'entre une densité réglementaire et la responsabilité individuelle. Dans ce but, une coopération continue et renforcée entre notamment les associations spécialisées, des organisations de patients, des préposés à la protection des données, est essentielle pour une réglementation spécifique, efficace et largement acceptée.

Vidéosurveillance sur le lieu de travail

—

Une société exploitant une boulangerie a déposé un recours au Tribunal cantonal contre le refus d'autorisation concernant l'installation d'une caméra de vidéosurveillance avec enregistrement qui filmait l'entrée du personnel. Le Tribunal cantonal a considéré qu'afin que la mesure de vidéosurveillance soit proportionnelle au but de sécurité visé, celui-ci doit être d'une importance élevée, c'est-à-dire visant la protection de la vie, de l'intégrité physique ou contre le vandalisme. La surveillance doit être adéquate en ce sens qu'elle atteint effectivement son but et doit être limitée à ce qui est nécessaire pour l'atteindre. En soi, l'installation litigieuse, qui couvre le parking et l'entrée du personnel, permet d'atteindre le but poursuivi car elle peut dissuader et permet de démasquer les auteurs d'infractions. Cependant, la mesure n'est pas proportionnelle au but recherché, pour plusieurs raisons. En effet, certains éléments filmés n'ont aucun rapport avec le but de sécurité, les images de la sortie des employés permettant de savoir quand ceux-ci arrivent et partent ou avec qui ils parlent ou partagent un véhicule. De plus, le système en question ne comporte pas de contrôle direct par des agents de sécurité habilités et le floutage des images n'écarte pas le risque d'atteinte à la personnalité des employés car ce procédé ne modifie que les côtés de l'image et non son centre. Enfin, les personnes non concernées doivent avoir la possibilité d'éviter le champ de la caméra sans qu'il y ait de passage obligé ni de surveillance dite totale. Ainsi, les caméras déjà présentes à l'intérieur du bâtiment suffisent à atteindre le but de prévention d'infractions, si bien que le retrait de la caméra filmant l'entrée du personnel n'enlève rien à l'effet dissuasif de l'ensemble. Le Tribunal cantonal a rejeté le recours (arrêt du Tribunal cantonal du 18 mai 2017, 601 2016 127).

Des données sensibles sur la santé pour tous?

La numérisation et les nouveaux développements technologiques concernent aussi les données sensibles sur la santé. «Quantified Self», une tendance à mesurer nos paramètres de santé, ou «Blockchain» ne sont que deux exemples de nouvelles technologies parmi tant d'autres. Qu'en est-il de la protection des données?

Les nouvelles technologies permettent de collecter toujours plus de données sur la santé. Qu'en advient-il? La comparaison entre les intérêts des consommateurs ou des patients et ceux des acteurs économiques est mise à rude épreuve. Le monde politique entend l'appel aux obligations sociales des données sur la santé. Le 22e Symposium on Privacy and Security a traité de ces questions en août à Zurich.

Le traitement des données est-il transparent?

Le traitement des données sur la santé ne s'effectue pas dans une zone de non-droit. Une première conférence a montré les nouvelles exigences du droit européen en matière de protection des données. Il s'agit de paramètres par défaut («privacy by default») ou de technologies favorables à la protection des données («privacy by design»). La législation fixe aussi de nouvelles obligations en matière d'information, de documentation et de déclaration (p. ex. en cas de violation des données). La Confédération et les cantons doivent adapter leurs législations sur la protection des données aux exigences du droit européen.
«Blockchain» est une base de données distribuée qui est assurée par cryptographie. Christian Cachin, chercheur en cryptographie et en informatique chez IBM, a présenté cette technologie dans son exposé et expliqué que la transparence augmente parmi les participants en raison de la large distribution de la base de données. En même temps, les données sont plus largement dispersées. Mais la protection des données et des droits de la personnalité est pratiquement inexistante et il n'y a pas de droit à l'oubli.
«Quantified Self – le soi quantifié» est en plein boom aujourd'hui. Les buts de ces diverses applications et technologies portables (téléphones intelligents, textiles intelligents, hearables, etc.) sont la mesure et le suivi de soi, une meilleure connaissance de soi, l'optimisation et la motivation. On distingue quatre grands domaines d'application: Smart Body, Smart Home, Smart Car et Smart Environment. C'est là qu'il y a un grand risque d'abus. Car ces applications permettent au fournisseur d'enregistrer le profil des utilisateurs. Mais ceux-ci ne sont souvent pas conscients de ce qu'il arrive à ces données. Comment le fournisseur les utilise-t-il, les revend-il et, si oui, à qui et à quelles fins? D'où la recommandation de Herrmann Kollmar, médecin et informaticien chez Medgate: «Restez maître de vos données».

Des normes et standards clairs

De nombreuses données sur la santé sont aussi collectées dans le cadre des rapports de travail, comme l'a révélé l'avocat Roger Rudolf. Le devoir d'assistance de l'employeur fixe néanmoins des limites au traitement des données. Elles ne peuvent être collectées que dans la mesure où elles sont nécessaires au déroulement technique et à la qualification.
Dans son exposé, la professeure Franziska Sprecher s'est opposée aux obligations sociales des données sur la santé. Il faut des normes et standards clairs et transparents qui permettent au patient de déterminer lui-même à qui il livre ses données, et lesquelles. Cela requiert sensibilisation et confiance en un traitement des données sûr et transparent.

Dictature numérique?

Les participants ont reconnu la nécessité d'aspirer à une sensibilisation et à une responsabilité numérique du citoyen. Celui-ci doit pouvoir décider en connaissance de cause à qui il confie ses données et à quelles fins il les transmet.
D'après Milosz Matuchek, juriste et journaliste, nous vivons aujourd'hui déjà dans une dictature numérique dont les conséquences ne sont toutefois pas visibles pour le citoyen. La numérisation est souvent perçue comme étant sans alternative. Pour s'affranchir de cette situation négative, il faut des critères clairs pour délimiter le progrès, des alliés, mais aussi une milice numérique.

Informations aux organes publics

Externalisation – Cloud

Les entreprises privées et les organes publics externalisent de plus en plus le traitement de leurs données. Cela signifie qu'ils ont recours aux services d'un tiers, à l'externe et contre rémunération, pour traiter des données qui étaient normalement assurés en interne. La plupart du temps, ils justifient cela par des raisons économiques. Or, avec l'interconnexion mondiale et l'utilisation de la mémoire virtuelle, de nombreuses questions se posent : l'organe qui externalise, sait-il où ses données sont localisées, si des sous-traitants interviennent, si une protection adéquate est assurée et s'il existe une réelle économie ? Pour être en droit d'externaliser, l'organe doit répondre aux obligations légales et notamment mettre en place toutes les mesures organisationnelles et techniques appropriées contre tout traitement non autorisé des données. En outre, il sera amené à répondre aux risques liés à l'externalisation dans la mesure où il demeure responsable des données.

La Commission de notre Autorité a rédigé une note relative à l'externalisation du traitement des données de l'Etat dans un Cloud en mettant en exergue tous les risques inhérents à cette externalisation et en citant les conditions strictes à respecter. Elle rappelle également que l'organe demeure responsable de ses données. Les organes publics doivent être transparents sur le traitement des données de leurs citoyens qui n'ont pas le choix de transmettre leurs données au Service des contributions, au Contrôle des habitants, à l'Etat civil, etc. En contrepartie, l'Etat doit leur garantir la sécurité de leurs données afin de préserver la confiance du citoyen. Enfin, la Commission relève qu'il ressort de l'expertise de Wolfgang Wohlers que la délocalisation des données sensibles, secrètes ou confidentielles dans un nuage à l'étranger serait assimilée à une violation du secret de fonction/professionnel.

Pour en savoir plus, voici le lien de la note y relative: http://intranet.fr.ch/intra/fr/intra/functions/toutes_les_actualites.cfm?fuseaction_pre=Detail&NewsID=62667

Adaptation de l'Ordonnance sur l'accès aux documents

Après l'entrée en vigueur de la modification de la Loi sur l'information et l'accès aux documents (LInf) au 1er janvier 2017, c'est au tour de l'Ordonnance sur l'accès aux documents (OAD) d'entrer en vigueur dans sa version adaptée le 1er janvier 2018. Désormais, toute la législation fribourgeoise dans le domaine de la transparence est conforme à la Convention d'Aarhus. Cette Convention, entrée en vigueur pour la Suisse le 1er juin 2014, octroie au public un droit d'accès aux documents environnementaux allant sur certains points un peu plus loin que celui qui était prévu de manière générale par la LInf.

L'introduction dans la loi du principe de l'interprétation conforme à la Convention d'Aarhus a permis de faire l'économie de plusieurs modifications de détail dans l'OAD. Certaines adaptations restaient toutefois nécessaires, d'abord parce que les modifications apportées par le législateur n'étaient pas limitées au seul domaine de l'environnement, mais aussi en raison des changements d'ordre procédural qui devaient être précisés au niveau de l'Ordonnance. De plus, quelques ajustements de l'Ordonnance tiennent compte de la pratique des six premières années d'application de la législation sur l'accès aux documents.

L'OAD ayant été conçue en fonction des notions d'organes publics au sens strict et de documents officiels, il a fallu introduire deux nouvelles dispositions permettant de faire le lien avec les notions nouvelles de personnes privées assimilées à des organes publics et d'information sur l'environnement. Egalement, l'attribution d'une compétence décisionnelle à l'Autorité cantonale de la transparence et de la protection des données et la question des délais spéciaux en lien avec les demandes d'accès à des informations sur l'environnement constituent des changements d'ordre procédural qu'il était nécessaire de concrétiser dans l'Ordonnance.

Parmi les ajustements qui visent à tenir compte de la pratique et à simplifier le travail des organes publics se trouve l'accès facilité aux documents ayant déjà fait l'objet d'une diffusion auprès du public. La notion de document achevé a été précisée de manière à ce qu'elle couvre également les documents émanant de tiers et la liste des exceptions à l'obligation de consulter les tiers concernés a été complétée et clarifiée. Finalement, une nouvelle disposition a été ajoutée qui concerne le devoir de collaboration des parties à la phase de médiation.

L'avant-projet mis en consultation durant l'été 2017 avait été dans l'ensemble bien accueilli, les modifications proposées étant globalement jugées nécessaires et pertinentes. Toutes les remarques émises ont fait l'objet d'un examen attentif de la part du groupe de travail et bon nombre d'entre elles ont été prises en considération d'une manière ou d'une autre.

Etude sur un identifiant personnel unique

Des données personnelles, souvent sensibles, sont conservées en Suisse dans plus de 14 000 registres tenus par des services administratifs ou d'autres organismes et indexés au moyen d'un identifiant unique, le numéro AVS. Ces systèmes informatiques peuvent faire l'objet d'attaques internes ou externes. Une nouvelle expertise de l'EPF de Zurich parvient à la conclusion que ces risques ne sont pas négligeables, car de nombreux systèmes informatiques d'écoles, d'administrations communales ou d'organisations non gouvernementales sont relativement peu sûrs. Elle recommande donc l'utilisation d'identifiants sectoriels, c'est-à-dire de pseudonymes non signifiants, et la création de processus d'identification associée à de nouvelles normes et à un contrôle efficace des liens. Vous trouverez l'expertise à l'adresse:
https://www.edoeb.admin.ch/aktuell/indexhtml?lang=fr.

Autorité cantonale de la transparence et de la protection des données ATPrD
Rue des Chanoines 2, CH-1700 Fribourg
T. +41 26 322 50 08, F + 41 26 305 59 72
-
www.fr.ch/atprd
-
Décembre 2017