EDOEB rapport-final-du-13-septembre-2010-concernant-les-données-biométriques-pour-un-s-2010-09-13 vom 13. September 2010

EDÖB, 2010-09-13, FR

Quelle: https://mcp.opencaselaw.ch/entscheid/edoeb_rapport-final-du-13-septembre-2010-concernant-les-données-biométriques-pour-un-s-2010-09-13

FR: EDOEB
rapport-final-du-13-septembre-2010-concernant-les-données-biométriques-pour-un-s-2010-09-13 du 13 septembre 2010

IT: EDOEB
rapport-final-du-13-septembre-2010-concernant-les-données-biométriques-pour-un-s-2010-09-13 del 13 settembre 2010

Erwägungen

E. 1
Point de départ

E. 4
Établissement des faits du 11 février 2010

E. 4.1
Personnes présentes

■ Président du CT XX ■ Avocat-conseil du CT XX ■ Consultant système du CT XX ■ 2 représentants du fournisseur du système ■ 2 collaborateurs du PFPDT

E. 4.2
Enrôlement biométrique

L'enrôlement est accompli de manière autonome par chaque membre. Les informations personnelles ainsi que le numéro d'adhérent figurent déjà dans la base des données des membres du club. L'adhérent introduit son numéro de membre sur le pavé numérique et présente son doigt sur le lecteur d'empreintes digitales. Le gabarit extrait de cette numérisation, comportant une douzaine de minuties, est mémorisé dans l'ordinateur local « PC biométrique » sous le numéro correspondant de membre et dans le format livré par le lecteur. Nous pensons qu'il s'agit plus d'un codage que d'un chiffrement et ne disposons en tous les cas d'aucune information probante (algorithme, clé, longueur) quant à un éventuel chiffrement.

Le système de réservations fonctionne sans cartes, de sorte que toutes les données sont mémorisées de manière centralisée. Les gabarits ne se trouvent cependant pas sur le même ordinateur que les autres données concernant les membres. Ces dernières se trouvent sur un PC au secrétariat (base de données des membres) et sur un serveur Web (données de réservation). Le PC biométrique est cependant relié par réseau sans fil (WLAN/WPA) au PC du secrétariat, qui est lui-même connecté à Internet (ligne ADSL). Les données brutes des empreintes digitales ne sont pas du tout conservées. Selon les dires du fournisseur de lecteurs biométriques, il n'est en outre pas possible de reconstruire les données brutes à

partir des gabarits mémorisés.

E. 4.3

Réservation d’un court de tennis

Avant de pouvoir jouer sur un court, il faut impérativement le réserver. Cette opération peut avoir lieu directement sur place ou alors préalablement depuis internet. La réservation doit ensuite être confir- mée au moyen de son empreinte digitale jusqu’à 10 minutes après le début de la rencontre. Tous les joueurs, à l’exception des invités, doivent confirmer leur participation avec leur empreinte digitale.

Pour ce faire, chaque joueur introduit son numéro de membre, avant d’être prié de présenter son doigt sur le lecteur biométrique. Le numéro de membre permet de retrouver automatiquement le gabarit de référence correspondant et de le comparer ensuite au gabarit présenté. Il s’agit donc bien d’une com- paraison biométrique 1-1 (vérification) et non pas d’une comparaison 1-n (identification) avec toutes les références contenues dans la base de données. La réservation est confirmée si tous les joueurs inscrits réussissent leur vérification biométrique ou simplement annulée dans le cas contraire. Dans ce dernier cas, le court apparaît alors comme „libre“ dans le système et peut à nouveau être réservé. Les joueurs peuvent être expulsés d’un court, si celui-ci n’est pas dûment marqué comme „réservé“.

Le système de réservation (serveur Web) produit des fichiers journaux sur les réservations, qui sont elles-mêmes bien sûr enregistrées. II est ainsi possible de consulter les réservations effectuées, soit l’utilisation des courts par les membres, de manière rétroactive pendant environ une année.

E. 4.4

Effacement des données

Les données personnelles des membres sont mémorisées à trois endroits: dans les fichiers de gaba- rits (PC biométrique), dans la base de données des membres (PC secrétariat) et dans le système de réservation (serveur Web). Selon les affirmations de l’informaticien du club, toutes les données peu- vent être détruites et ce à n’importe quel moment. Cependant, aucun délai de conservation ne serait pour l’instant prescrit, ceci étant dans le domaine de responsabilité du CT XX.

Lorsqu’un membre quitte le club, son gabarit peut simplement être détruit. Dans le système de réser- vation, les données principales sont détruites par les informaticiens tous les 2 à 3 ans et les fichiers journaux après environ 1 an, avant tout pour gagner de la place. L’administration du CT XX n’effectue elle-même aucun effacement régulier de données.

Le PFPDT a rendu attentif sur place au fait que le principe de proportionnalité des traitements de don- nées impose un effacement aussi rapide que possible des données, et soulignons que le CT XX de- vrait introduire des règles pour un effacement approprié des données.

E. 4.5

Devoir d’information et droit d’accès

Les membres ont été préalablement informés dans le cadre de la votation sur le système planifié lors de la dernière AG. Une discussion a eu lieu suite à cette assemblée, discussion au cours de laquelle d'autres informations ont été échangées. Après la décision d'introduire ce système, tous les membres ont en outre été informés au sujet de ce système par poste, courriel et le magazine du club. Il n'existe par contre pas d'information standardisée pour les nouveaux membres. Le président s'engage à amé- liorer l'information aux membres, sur requête du PFPDT.

Les membres peuvent en tout temps s'adresser au président du club pour consulter leur gabarit. Sur proposition du PFPDT, le président s'est engagé à étendre ce droit d'accès à la base de données des membres et au système de réservations.

E. 4.6

Alternatives à la saisie biométrique

Le système permet d'effectuer une réservation à l'aide d'un code personnel (PIN) au lieu d'une em- preinte digitale. Les personnes qui ne peuvent ou ne désirent pas utiliser le système biométrique ont ainsi la possibilité d'éviter ce système. Cette alternative est pour l'instant utilisée par une dizaine de personnes. Sur demande expresse du PFPDT, le président s'est déclaré d'accord, d'informer à l'avenir les membres de manière transparente sur cette voie alternative.

E. 4.7

Avantages du système de reconnaissance biométrique

L'installation du CT XX se compose principalement des courts de tennis et du clubhouse avec vestiai- res et restaurant. Une réception ou quelque chose de comparable n'existe pas. C'est pour cette raison qu'un contrôle automatisé des ayants droits doit avoir lieu.

Le système de réservations fonctionnait jusqu'à présent à l'aide de codes personnels. Le problème rencontré était que certains PINs ont été ébruités et ainsi utilisés par plusieurs personnes externes au club. Le système a donc dû être modifié, de façon à ce qu'une vérification univoque avec un coût aus- si faible que possible (les moyens financiers du club seraient modestes selon les dires du président) soit introduite. La vérification à l'aide d'empreintes digitales offre ces possibilités, raison pour laquelle elle a été choisie. Le club a vécu depuis lors une croissance sensible du nombre des membres, et les courts sont néanmoins moins surchargés qu'auparavant. Cela laisse à penser, que les abus du sys- tème précédent étaient significatifs.

On s'est consciemment décidé pour un système sans cartes personnelles. Les cartes peuvent en effet facilement être oubliées ou perdues, ce qui d'une part augmente le risque d'abus et d'autre part crée un désagrément supplémentaire pour les membres. La majorité des membres salue la solution sans cartes, car celle-ci serait bien plus confortable (« on a toujours ses doigts avec soi… »). Le système serait accepté par une large majorité des membres et on serait satisfait de cette solution.

E. 4.8

Communication de données à des tiers (externes)

Aucune donnée biométrique n’est communiquée à des tiers. Aucun transfert de ces données n’a lieu vers le fournisseur de lecteur biométrique, le système n’étant pas relié à cette entreprise.

Le système de réservations (sans données biométriques) est par contre consultable sans aucune forme de mot de passe à partir du site du club. Chaque internaute peut ainsi voir, qui a réservé quel court à quel moment, et ce de manière rétroactive pendant 2 à 3 ans. Chaque membre du club peut certes demander à modifier son nom d’utilisateur lors de la création de son compte et définir ainsi un pseudonyme, en particulier pour ce type d’affichage, plutôt que son identité réelle. Par défaut, le sys- tème retient la première lettre du prénom suivie des 20 premières lettres de son patronyme.

E. 4.9

Localisation des ordinateurs, sécurité des données

Les gabarits sont mémorisés sur un ordinateur (PC biométrique) qui se trouve dans une antichambre du clubhouse. Ce local est sécurisé avec une porte normale munie d’une simple serrure, dont les dé- tenteurs de clé sont : le président, le resp. informatique, l’intendant et 2-3 autres personnes. Sur une tablette à l’extérieur du local, cette borne offre aux utilisateurs les périphériques suivants : un pavé numérique pour introduire le numéro d’adhérent, un lecteur d’empreintes digitales et une souris per- mettant de déplacer le curseur sur l’écran et de cliquer sur la fonction désirée.

Les données des membres se trouvent sur un PC dans le secrétariat du club, situé au premier étage du clubhouse et accessible de l’extérieur par une galerie. Le secrétariat est également fermé par une porte normale munie d’une simple serrure et peut être visité par n’importe qui durant les heures d’ouverture. En dehors de celles-ci, le secrétariat est accessible aux détenteurs de clé suivants : le président, le resp. informatique, l’intendant, 4 membres du comité et 4 professeurs employés par le club. L’accès logique au PC administratif du secrétariat est cependant protégé par mots de passe. Notons encore que ce PC administratif a accès aux gabarits par le biais d’un partage caché qui a été

créé sur le PC biométrique. Pour augmenter la sécurité de cet accès, il a été suggéré de créer un profil particulier pour cette gestion.

Le système de réservations se trouve sur un serveur Web du fournisseur. L’accès aux données des personnes de la base de données est protégé par le mot de passe de l’administrateur du système. Nous ne connaissons par contre pas les conditions contractuelles de sécurité des données offertes par le fournisseur.

Les PC bénéficient tous deux d’un accès à Internet et ils communiquent entre eux par un réseau sans fils. Ce WLAN protégé pour l’instant par le protocole WPA (et dès mars 2010 par WPA2) peut être utilisé pour accéder à Internet aux alentours du clubhouse par tous les membres qui le désirent. Il leur suffit pour ce faire de demander le mot de passe d’accès.

Les données traditionnelles des membres sont enregistrées en texte clair, tandis que les gabarits sont mémorisés prétendument sous une forme chiffrée. Nous pensons cependant qu’il s’agit plus d’un co- dage (ASN.1 DER) que d’un chiffrement et ne disposons en tous les cas d’aucune information pro- bante (algorithme, clé, longueur) quant à un éventuel chiffrement.

E. 4.10

Maintenance du système

La maintenance du système est assurée par les informaticiens du CT XX. Grâce à leur co- dage/chiffrement, les gabarits ne peuvent pas être décodés dans le cadre des travaux de mainte- nance, à la différence des autres données mémorisées sous une forme claire.

5. Jugement du point de vue de la protection des données

E. 5.1

Données biométriques en tant que données personnelles

E. 5.1.1

Point de départ

La loi fédérale sur la protection des données du 19 juin 1992 (LPD; RS 235.1) est applicable dans chaque cas où des données personnelles au sens de l'art. 3 lit. a LPD sont traitées. Dans le cas pré- sent, des données biométriques (gabarits d'empreintes digitales) sont traitées pour la réservation de courts de tennis.

E. 5.1.2

Jugement du point de vue du PFPDT

Des données biométriques d'empreintes digitales sous forme de gabarits biométriques (données de référence) rendent une personne identifiable par comparaison avec une empreinte digitale présentée ultérieurement. Les données biométriques peuvent ainsi servir à authentifier/vérifier (resp. identifier) une personne. L'identifiabilité ne découle pas seulement de cette possibilité de comparaison biométri- que, mais aussi par le fait qu'il existe une correspondance entre la base de données des gabarits (PC biométrique) et celle des membres (PC secrétariat). Par cette correspondance, les données biométri-

ques sous forme de gabarits peuvent clairement être mises en relation avec une personne et la rendre ainsi identifiable (art. 3 lit.a LPD).

Dans le cas du CT XX, une douzaine de minuties extraites d'une empreinte digitale sont mémorisées. Les données de ces minuties sont en fait codées (et comprimées) au moyen d'un algorithme mathé- matique. Les algorithmes d'extraction de gabarits à partir de données biométriques brutes sont de nos jours ni standardisés, ni transparents. Il est de ce fait difficile de pouvoir évaluer formellement et défi- nitivement la sensibilité (éléments sur la santé/race) d'un gabarit biométrique. De plus, les données biométriques brutes ou dérivées rendent une personne identifiée ou identifiable, tandis que leur col- lecte – en particulier celle des empreintes digitales – laisse en général des traces. La collecte de don- nées biométriques brutes ou dérivées est ainsi susceptible de permettre la création d'un profil de mouvement de la personne concernée. En conséquence, il existe un potentiel élevé d'atteinte aux droits de la personnalité lors de la collecte de données biométriques. On doit par ailleurs constater, que le Conseil de l'Europe et le groupe de l'article 29 de l'UE (Directive 95/46/EC du Parlement euro- péen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) reconnaissent pour les mêmes raisons le caractère sensible des données biométriques.

E. 5.2
But du traitement de données

E. 5.2.1
Point de départ

Chaque traitement de données personnelles peut entraîner une atteinte au droit à la protection de la sphère privée selon l'art. 13 al. 2 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.; RS 101). De ce fait, un tel traitement nécessite un motif justificatif particulier. Des considé- rations pratiques ou une simple convivialité pour les clients ne représentent essentiellement pas un motif justificatif suffisant pour le traitement de données biométriques.

Selon les indications du CT XX, la saisie des données biométriques n'a pour seul but, que d'empêcher les abus d'utilisation des courts de tennis par des personnes non autorisées. Avant l'introduction du système biométrique de réservation, les courts étaient réservés au moyen d'un NPI, ce qui s'est révé- lé être propice aux abus. Les codes ont été en partie transmis et utilisés par plusieurs personnes (non-membres). Ceci n'est plus possible avec le nouveau système biométrique. Le CT XX a par la suite aussi remarqué une hausse significative du nombre de membres, tandis que les courts étaient quant à eux moins fréquentés.

On a volontairement renoncé à l'utilisation de cartes individuelles de membre, car il y a le risque que les cartes soient perdues ou oubliées. C'est pour ces raisons de confort que les membres ont préféré un système biométrique sans carte.

E. 5.2.2
Jugement du point de vue du PFPDT

Le nouveau système de réservation et la collecte conséquente de données biométriques poursuivent des finalités plausibles. Pour le PFPDT, on doit cependant se poser sérieusement la question de sa- voir s'il n'existe pas des alternatives pour éviter les abus qui porteraient moins atteinte aux droits de la personnalité des personnes concernées (cf. à ce sujet les remarques générales concernant la propor- tionnalité au chiffre 5.5).

E. 5.3
Licéité du traitement de données / Consentement des per- sonnes concernées

E. 5.3.1
Point de départ

Les données biométriques sont des données personnelles au sens de la LPD, dont le traitement re- quiert un motif justificatif (art. 12 et 13 LPD). Dans le cas présent, le consentement des personnes concernées peut être retenu comme motif justificatif.

Selon les informations du CT XX, le système prévu a fait l'objet d'une discussion de principe lors d'une assemblée générale. Lors de la votation qui a suivi, la majorité des membres présents s'est prononcé en faveur de l'introduction d'un tel système biométrique. Le système a ensuite été introduit et une notice d'utilisation du système de réservation a été publiée sur le site resp. sur la « borne ». Toujours selon les informations du CT XX, les

nouveaux membres sont informés oralement par le président sur le système de réservation biométrique.

Il n'existe manifestement aucun enregistrement écrit concernant les informations remises aux mem- bres lors de l'AG qui a ratifié l'introduction de ce système. On doit cependant partir de l'idée que les informations transmises n'étaient que de nature globale et ne renseignaient en particulier pas sur les modalités de traitement de données (par ex. nature et lieu de stockage des gabarits, durée de conser- vation, protection d'accès) dans le cadre du système biométrique de réservation.

La notice d'utilisation du système de réservation n'aborde que très superficiellement les modalités de traitement du système biométrique. Elle ne renseigne principalement que sur la procédure d'enrôlement et de réservation.

L'information orale du président a lieu à chaque fois de manière individuelle et n'est donc pas stan- dardisée. On peut ici aussi partir de l'idée que le président n'informe pas au sujet des modalités de traitement.

D'autres supports d'information n'existent pas pour l'instant, mais ils devraient selon le CT XX être créés et remis aux membres du club.

Toutes les personnes qui ne peuvent ou ne veulent pas utiliser le système biométrique de réservation, peuvent effectuer la réservation à l'aide d'un NPI comme jusqu'à présent. Jusqu'à présent, environ 10 personnes ont fait usage de cette possibilité. Les membres ne sont pas informés au préalable de cette alternative. L'alternative n'est proposée qu'au moment où quelqu'un refuse de saisir ses données biométriques ou s'il s'avère que le système biométrique est dans l'incapacité d'enrôler la personne concernée.

E. 5.3.2

Jugement du point de vue du PFPDT

Du point de vue du PFPDT, le consentement de la personne concernée requiert des exigences sévè- res quant à sa mise au courant, en particulier dans un domaine aussi sensible que celui du traitement d'empreintes digitales. Il faut donc exiger que les membres soient informés plus concrètement sur les modalités de traitement, afin qu'ils soient au clair quant à la portée de leur consentement. Par consé- quent, il faut communiquer aux personnes concernées les points essentiels du traitement de données, comme où et pour combien de temps les données biométriques sont mémorisées, que se passe-t-il avec les gabarits et les données de journalisation, qui possède les droits d'accès aux données et à qui

ils peuvent, si jamais, être transférés. Tout cela devrait avoir lieu par le biais d'une feuille d'information standardisée qui devrait être distribuée à tous les membres existants ainsi qu'aux nouveaux. Cette feuille d'information doit être signée par l'administration et dotée d'un marquage de contrôle de ver- sion. Les membres doivent en outre être informés de l'existence de l'alternative (présentement la ré- servation par NPI), afin que le consentement ait lieu librement et pas sous la présupposition que l'on n'a pas le choix.

Les membres ne disposaient pas au moment de la votation de l'assemblée générale des connaissan- ces nécessaires de l'état de faits leur permettant de donner un consentement juridiquement accepta- ble. De plus, on doit à ce stade encore préciser que seul le consentement individuel de chaque per- sonne concernée peut justifier l'atteinte aux droits

de la personnalité. Une décision majoritaire lors d'une AG ne remplit pas cette exigence.

On doit aussi partir de l'idée qu'à l'heure actuelle, les membres ne sont pas suffisamment informés sur les modalités de traitement pour pouvoir consentir valablement au traitement de données. Un consen- tement valable ne peut être vérifié qu'au moment où les exigences formulées ci-dessus sont remplies et les membres se décident pour le système biométrique de réservation en parfaite connaissance de ces informations.

E. 5.4

Traitement selon la bonne foi / Transparence

E. 5.4.1

Point de départ

Le traitement de données personnelles doit être effectué conformément au principe de la bonne foi (art. 4 al. 2 LPD). Cela signifie d'une part que le traitement doit être transparent pour la personne con- cernée et d'autre part que la collecte et chaque autre traitement de données doit être en principe re- connaissable pour la personne concernée.

Comme déjà mentionné au chiffre 5.3, les membres ont été informés après l'AG sur la collecte de données biométriques au moyen de la notice d'utilisation du système de réservation, ainsi qu'oralement par le président du club. Une feuille d'information standardisée n'existe cependant pas. L'enrôlement est effectué par le membre lui-même. Ce dernier doit donc agir activement pour que ses données biométriques puissent être saisies (glissement de son doigt sur le senseur biométrique de la « borne » près de l'entrée du clubhouse). Aucune donnée biométrique ne peut donc être collectée sans sa participation.

E. 5.4.2

Jugement du point de vue du PFPDT

Comme les données biométriques ne peuvent être collectées sans participation de la personne con- cernée, le traitement de ces données a bien lieu d'une manière reconnaissable. Pour un traitement de données aussi transparent que possible, il faudrait remettre aux membres, en plus des informations actuellement communiquées oralement, une feuille d'information standardisée sur laquelle est décrit tout ce qui passe avec les données personnelles. Cette feuille peut se référer à ce qui est écrit au chiffre 5.3.

E. 5.5

Proportionnalité du traitement de données

Le traitement de données personnelles doit être effectué conformément au principe de la proportion- nalité (art. 4 al. 2 LPD). Cela signifie que celui qui traite des données ne peut traiter que celles dont il a effectivement objectivement besoin pour un but déterminé et qui sont en relation raisonnable avec la finalité du traitement et avec l'atteinte à la personnalité.

E. 5.5.1

Proportionnalité matérielle – Point de départ

Un traitement de données n'est proportionnel que s'il se limite au contenu absolument nécessaire pour atteindre le but fixé. La proportionnalité matérielle demande de ménager le plus possible l'utilisation de données personnelles. Cela impose aussi qu'aucune donnée

excédentaire non indis- pensable au but poursuivi ne soit produite. Il est également irrecevable de collecter de manière provi- sionnelle des données personnelles, à moins que le but poursuivi ne l'exige impérativement.

Avec l'introduction du nouveau système de réservation, des gabarits biométriques sont générés à partir des empreintes digitales des membres, puis stockés dans une base de données centralisée. Les données biométriques brutes (i.e. l'image originale de l'empreinte digitale) ne sont pas conser- vées. Le système fonctionne sans cartes individuelles. Une réservation préalable d'un court à partir du système de réservation en ligne ou de la „borne biométrique" est confirmée par la saisie du numéro de membre suivie de l'apposition du doigt sur le lecteur biométrique. Le gabarit extrait du doigt présenté est comparé avec le gabarit de référence correspondant au numéro de membre introduit. Si les deux gabarits concordent, la réservation est confirmée et reste mémorisée et consultable dans le système de réservation pour les 2-3 prochaines années. Si les deux gabarits ne concordent par contre pas, la réservation n'est alors pas confirmée et radiée 10 minutes après le début de la période de réservation.

À côté des gabarits biométriques, d'autres données sur les membres (renseignements personnels, données sur les joueurs, etc.) sont conservées dans le PC du secrétariat et les données de réserva- tion bien sûr dans le système der réservation. Les données de réservation sont consultables sans mot de passe sur Internet par n'importe quel internaute. Le nom d'utilisateur (par défaut la première lettre du prénom suivie au maximum des 12 premières lettres du nom de famille) et les périodes de réserva- tion sont consultables pour les 2-3 années passées. Pour effectuer une réservation en ligne, le mem- bre doit se connecter à l'aide de son nom d'utilisateur et de son mot de passe. Le nom affiché peut être modifié par le membre lui-même lors de son inscription.

E. 5.5.2

Jugement de la proportionnalité matérielle du point de vue du PFPDT

E. 5.5.2.1

Centralisation des données biométriques

La mise en œuvre de processus biométriques dans le domaine privé représente en fonction de leur conception dans le cas concret une atteinte plus ou moins intensive aux droits de la personnalité des personnes concernées. Avant la mise en œuvre de tels processus biométriques, il faut donc en prin- cipe toujours vérifier si d'autres mesures appropriées, mais moins attentatoires aux droits fondamen- taux des personnes concernées, ne permettraient pas également d'atteindre le but visé. Par ailleurs, il faut déjà lors du choix et de la conception du processus biométrique veiller à choisir un système qui soit le plus économique possible en données et qui reste dans un rapport raisonnable avec le but visé. Comme le Groupe de l'art. 29 de l'UE le stipule dans sa prise de position sur la mise en œuvre de la biométrie, „les risques pour la protection des droits et libertés fondamentaux de l'individu, avant tout la question de savoir si le but visé ne pourrait pas être atteint d'une manière moins attentatoire aux droits de la personne concernée, doivent aussi être pris en considération„ lors de l'appréciation de la propor-

tionnalité. Comme le même groupe le stipule encore „les systèmes biométriques utilisés pour le contrôle d'accès (vérification) comportent moins de dangers pour la protection des

droits et libertés fondamentaux de l'individu, lorsqu'ils se basent sur des caractéristiques corporelles ne laissant pas de trace (par ex. contour de la main, mais pas empreinte digitale) ou qu'ils exploitent des caractéristiques corporelles laissant bien des traces, mais mémorisent les données biométriques sur un support qui reste en possession de la personne concernée (en d'autres termes lorsque les données ne sont pas enregistrées dans l'appareil de contrôle d'accès ou dans une base de données centralisées [Groupe de travail « Article 29 » sur la protection des données, Document de travail sur la biométrie, adopté le 1er août 2003, 12168/02/FR GT 80]).

Dans le cas présent, il s'agit d'un système de réservation pour une installation de loisirs. La biométrie est mise en œuvre pour la vérification des membres du club. On n'atteint une économicité de données qu'en collectant les données biométriques absolument nécessaires à la vérification. Les données bru- tes ne sont pas nécessaires pour la vérification. La comparaison avec un gabarit suffit pour vérifier si la personne est autorisée lors de la confirmation de réservation. Le fait de n'enregistrer que les gaba- rits biométriques, comme cela est effectué par le CT XX, est donc proportionnel du point de vue de l'économicité de données.

Les données biométriques sont liées de manière permanente aux personnes. Précisément lorsqu'ils s'agit de domaines aussi sensibles que les empreintes digitales, ces données biométriques devraient de ce fait être mémorisées dans le domaine d'influence de la personne concernée, c'est-à-dire du membre, et y rester.

De ce qui a été dit jusqu'à présent, il découle qu'il existe les trois variantes suivantes pour une réalisa- tion du système conforme à la protection des données dans le cadre de la mise en œuvre de la bio- métrie pour vérifier les personnes autorisées à accéder à une installation de loisirs. Pour des caracté- ristiques laissant des traces (physiques ou numériques) comme les empreintes digitales ou les photo- graphies du visage, seules les variantes a) et b) avec cartes individuelles garantissent un niveau de protection suffisant. La variante c) sans carte est par contre envisageable pour des caractéristiques biométriques ne laissant pas de trace comme le réseau veineux du doigt ou le contour de la main.

a) Décentralisation : (sur cartes)

Comme le PFPDT le stipule dans son guide concernant les systèmes de reconnaissance biométrique datant de septembre 2009, la protection de la personnalité des personnes concernées est au mieux assurée lors de la mise en œuvre de la biométrie dans le domaine privé, si

1. les données biométriques sont conservées sous forme de gabarits chiffrés sur un support sé- curisé se trouvant sous contrôle individuel de la personne concernée ; et 2. la personne concernée doit libérer explicitement et consciemment chaque accès aux don- nées ; et 3. la vérification de l'identité n'a lieu que sur le support sécurisé, de telle sorte que les données biométriques ne quittent à aucun moment l'environnement sécurisé du support et le contrôle de la personne concernée (comparaison biométrique sur carte, cf. guide p. 13).

b) Pseudodécentralisation : (avec cartes)

Un niveau approximativement aussi élevé quant à la protection de la personnalité peut être atteint au moyen d'une pseudodécentralisation. Cette solution a aussi été esquissée par le Tribunal administratif fédéral dans son jugement du 4 août 2009 (A-3908/2008) concernant le cas KSS. À la différence de la

vraie décentralisation, les données biométriques sont certes mémorisées de manière centralisée, mais un accès logique à ces données n'est possible qu'à l'aide d'un code de correspondance mémo- risé sur une carte possédée exclusivement par la personne concernée. Cela signifie en détail ce qui suit :

1. les données biométriques sont conservées de manière centralisée sous forme de gabarits chiffrés (et non de données brutes comme une image ou une photographie) ; 2. les gabarits biométriques sont conservés de telle sorte qu'aucun lien avec une personne iden- tifiée ou identifiable ne puisse être établi par le maître de fichier. Des données statistiques ou accessoires peuvent leur être associées, pour autant quelles ne soient pas identifiantes ; 3. le lien entre un gabarit biométrique et la personne concernée est établi uniquement avec l'autorisation expresse et libre de cette dernière lorsqu'elle fait usage de sa carte individuelle .

c) Centralisation : (sans carte)

Dans le cas où l'introduction de cartes individuelles n'est pas souhaitée dans le cadre d'une vérifica- tion biométrique des membres d'un club de loisirs, seule un système avec une centralisation des réfé- rences biométriques est envisageable. Comme de tels systèmes sont théoriquement appropriés pour accomplir une identification biométrique, ils doivent respecter l'ensemble des conditions suivan- tes pour ne pas être jugés disproportionnés pour effectuer une pure vérification biométrique :

1. seules des caractéristiques biométriques sans trace (physique ou numérique) peuvent être exploitées ; 2. les données biométriques sont conservées de manière centralisée sous forme de gabarits chiffrés (et non de données brutes comme une image ou une photographie) ; 3. les gabarits biométriques sont conservés de telle sorte qu'aucun lien avec d'autres données identifiantes de personnes concernées ne puisse être établi par le maître de fichier. Des don- nées statistiques (ex : sexe) ou accessoires (ex : date d'expiration) peuvent cependant leur être associées, pour autant qu'elles ne soient pas identifiantes ; 4. le lien entre un gabarit biométrique et la personne concernée est établi de manière volatile par le système de reconnaissance, uniquement pour attester de son appartenance aux membres. La suite des opérations (confirmation de réservation…) a lieu sur une base non biométrique.

En conclusion, le CT XX doit pour l'avenir choisir une des trois variantes décrites ci-dessus et la met- tre en œuvre de manière appropriée, aussi pour les données déjà mémorisées de manière centrali- sée. La centralisation actuelle des données biométriques dans le cas présent de la réservation de courts de tennis par le CT XX est disproportionnée du point de vue du principe de l'économicité des données et du principe du traitement ménageant au mieux les données personnelles.

E. 5.5.2.2

Publication des données de réservation sur Internet

Le système de réservation permet aux membres de procéder à la réservation des courts depuis Inter- net et de confirmer ensuite cette réservation sur place avec son empreinte digitale. C'est dans ce but que le système est activé sur le site du CT XX. Le PFPDT reconnaît que la réservation en ligne est d'une grande utilité pour les membres et offre par ailleurs la possibilité de rechercher et trouver des partenaires de jeu. Pour atteindre cette finalité, il paraît aussi proportionnel de mettre à disposition des membres cet accès en ligne

au système de réservation.

15/27

Du point de vue du PFPDT, il n’y a par contre aucune raison d’autoriser sans restriction cet accès aux données de réservation et de permettre ainsi leur consultation par des non-membres. Cela dépasse de loin ce qui est nécessaire pour atteindre le but visé. Le PFPDT est donc d’avis que l’accès en ligne au système de réservation doit être restreint aux seuls membres du club. Une protection par mot de passe pourrait par exemple suffire. Du fait que la réservation en ligne requiert de toute façon une connexion, cette restriction ne nécessiterait qu’une modification minimale du système. On pourrait par exemple déjà exiger une connexion pour la consultation des données de réservation.

Lors de la création d’un compte d’utilisateur, le PFPDT suggère en outre qu’il soit automatiquement mentionné que le véritable nom de famille sera affiché par défaut dans le système de réservation en ligne et qu’on demande explicitement à la personne concernée s’il est d’accord avec cette pratique ou si elle préfère recourir à la possibilité de pseudonymisation du nom affiché.

En résumé, on peut constater que la publication actuelle des données de réservation sur Internet dé- passe de loin ce qui est nécessaire pour atteindre le but poursuivi. Elle n’est donc pas proportionnelle par rapport au principe du traitement ménageant au mieux les données personnelles.

E. 5.5.3

Proportionnalité temporelle – Point de départ

L’exigence de proportionnalité limite également le traitement de données sur l’échelle temporelle. Dès que les données personnelles ne sont plus utiles pour le but poursuivi, elles doivent être détruites ou anonymisées. Il faut prévoir à cet égard une destruction ou une anonymisation le plus rapidement possible.

Actuellement, des données personnelles sont enregistrées à trois endroits : sur le PC « biométrique », sur le PC du secrétariat et sur le serveur web du système de réservation. Un règlement pour la durée de conservation ou la responsabilité de destruction n’existe pour aucun de ces endroits. Jusqu’à pré- sent, aucune destruction régulière de données n’est effectuée sur le PC „biométrique“ et sur le PC du secrétariat, les données de réservation du système der réservation sont par contre détruites tous les 2-3 ans pour des raisons de place, tandis que les données de journalisation sont effacées après envi- ron une année.

E. 5.5.4

Jugement de la proportionnalité temporelle du point de vue du PFPDT

Le PFPDT a déjà rendu attentif lors de la visite des installations sur place au fait que la durée de conservation et la responsabilité pour la destruction des données (en particulier sensibles) plus né- cessaires devaient être réglées et consignées dans un règlement, car il n’est sinon pas possible pour les personnes concernées d’estimer la durée de conservation des données. Il existe en outre le dan- ger effectif que la destruction des données ne soit pas suffisamment prise en considération et que celles-ci soient éternellement conservées.

Les gabarits sur le PC „biométrique“ et les données des membres sur le PC du secrétariat doivent être détruites dès qu’elles ne sont plus nécessaires. Cela est au plus tard le cas lorsqu’un membre donne sa démission. La destruction des données lors d’une démission

doit par conséquent d’une part être arrêtée dans le règlement et d’autre part être enregistrée dans les processus standard pour de tels cas. Pour le PFPDT, il n’y a en apparence aucune raison qui justifierait une durée de conservation de 2-3 ans pour les données de réservation et d’un an pour les données de journalisation du système de réservation.

16/27

Le PFPDT estime donc que les durées de conservation sont disproportionnellement longues et doi- vent être réduites à une mesure appropriée. Le CT XX doit ainsi faire une proposition au PFPDT pour déterminer comment les délais de destruction doivent être fixés et comment ces délais sont ensuite (techniquement) mis en œuvre. À part la destruction des données mentionnées ci-dessus, il faut aussi régler celle des sauvegardes existantes de ces données.

E. 5.6

Finalité du traitement

E. 5.6.1

Point de départ

Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par la loi ou qui ressort des circonstances (art. 4 al. 3 LPD). Comme une modification du but du traitement n’est pas contrôlable par les personnes concernées à cause de la centralisation des données biométriques, il faut privilégier des solutions techniques qui garantissent suffisamment le respect de la finalité.

E. 5.6.2

Jugement du point de vue du PFPDT

De par la centralisation actuelle des gabarits biométriques, on ne peut pas totalement exclure un dé- tournement de finalité lors du traitement de ces données. Cela est entre autre possible, car les don- nées ne se trouvent pas dans la sphère d’utilisation des personnes concernées. Un détournement de finalité par liaison avec d’autres fichiers ou par communication à un tiers externe serait possible. Même si on tient compte du fait qu’aucunes données brutes mais uniquement des gabarits biométri- ques sont stockés dans la base de données, on doit également renoncer à la mémorisation actuelle centralisée des données biométriques à cause du principe de finalité et choisir une des variantes mentionnées au chiffre 5.5.2.1.

E. 5.7

Exactitude des données (fiabilité, applicabilité)

E. 5.7.1

Point de départ

Le processus de comparaison entre données de référence et données présentées (ici des gabarits d’empreintes digitales) se base sur un calcul de probabilités et fournit une valeur de concordance, qui doit être supérieure à un seuil prédéfini, pour que la personne soit reconnue. De cette seule valeur de seuil dépendent les deux taux „False Rejection Rate (FFR)“ et „False Acceptance Rate (FAR)“ de manière inversement proportionnelle. Pour des motifs de protection de la personnalité, on devrait mi- nimiser avant tout le FAR, sans cependant trop fortement péjorer le FRR. Le choix d’une valeur opti- male du seuil

d’acceptation pour atteindre une fiabilité suffisante du système biométrique global n’est donc pas facile à effectuer.

Il ne faut également pas négliger le fait que certains utilisateurs (à cause de membres manquants, blessures, cicatrices ou à cause de leur jeunesse/vieillesse) ne présentent pas de caractéristiques biométriques (ou alors de qualité insuffisante) pour accomplir une telle vérification. Pour ces person- nes, un scénario alternatif doit être prévu, sans que cela puisse conduire à une discrimination des personnes concernées.

E. 5.7.2

Jugement du point de vue du PFPDT

Pour des raisons de protection des données, le taux FAR devrait être minimisé, sans pour autant trop péjorer le taux FRR. Un seuil d’acceptation optimal doit en outre être choisi. Chaque système biomé- trique présente un certain taux (non nul) de FAR. La vérification ne peut de ce fait avoir lieu de ma- nière entièrement fiable. Le système du CT XX extrait 12 minuties par gabarit biométrique, ce qui est à nos yeux tout juste suffisant. Des tests sur place ont néanmoins démontré que le système fonc- tionne pour l’instant à satisfaction.

Des problèmes apparaissent parfois aussi auprès de personnes dont certaines caractéristiques bio- métriques manquent ou ne sont que difficilement lisibles (enrôlement). Pour de telles exceptions, il faut planifier et mettre en œuvre une applicabilité équivalente du système de reconnaissance. Une telle alternative existe dans le cas présent. Au lieu d’une vérification au moyen d’empreintes digitales, un NPI est utilisé. Cette alternative est pour les personnes concernées équivalentes aussi bien du point de vue du coût que de celui de la manipulation. Il y a manifestement déjà des membres qui ne veulent ou ne peuvent pas utiliser le système biométrique et confirment par conséquent leurs réserva- tions à l’aide d’un NPI. Cela fonctionne sans problème.

L’exactitude des données est ainsi assurée par le système de réservation. Le PFPDT n’a ici pas d’autres remarques.

E. 5.8

Sécurité des données

E. 5.8.1

Point de départ

Selon l’art. 7 LPD, les données personnelles doivent être protégées contre tout traitement non autori- sé par des mesures organisationnelles et techniques appropriées. Il faut en particulier garantir la con- fidentialité, la disponibilité et l’intégrité des données personnelles. Ces exigences ne sont plus satisfai- tes, si des personnes non autorisées peuvent aisément accéder aux données ou si un appareil étran- ger peut capturer ou manipuler ces données. La sécurité des données est sous la responsabilité de l’organisme qui possède la maîtrise sur les données personnelles (art. 8 al. 1 de l’ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (OLPD; RS 235.11).

Comme déjà mentionné, le PC „biométrique“ et le PC du secrétariat se trouvent chacun dans un local du clubhouse accessible depuis l’extérieur et protégé seulement par un simple cadenas. 5-6 person- nes ont un accès physique au PC „biométrique“, toutefois 2-3 d’entre

elles n’ont pas pu être nommées précisément. 11 personnes ont un accès physique au PC du secrétariat en dehors des heures d’ouverture, tandis que quiconque peut pénétrer dans le bureau pendant les heures d’ouverture, le PC n’étant en principe pas laissé sans surveillance et l’accès logique aux données qu’il contient étant protégé par mot de passe.

Le PC „biométrique“ et le PC du secrétariat, au bénéfice d’un accès Internet (ADSL), sont reliés entre eux par un réseau sans fil (WiFi). Le réseau WiFi est sécurisé par le protocole WPA (WPA2 depuis mars 2010). Le mot de passe WiFi est communiqué aux membres qui le demandent, afin que ceux-ci puissent accéder à Internet depuis leur téléphone ou ordinateur pendant leur séjour sur le terrain du club.

À partir du PC du secrétariat, il est possible d’accéder aux gabarits biométriques par le biais d’une partition partagée cachée sur le PC « biométrique ».

E. 5.8.2

Jugement du point de vue du PFPDT

Le PFPDT juge insuffisante la protection physique du PC „biométrique“ et du PC du secrétariat. Les portes y compris les cadenas peuvent être forcés sans grand effort. Les deux PC ne sont ainsi pas physiquement sécurisés comme ils devraient l’être, et un vol de données ou même d’un boîtier PC complet serait facilement envisageable. Cela doit être pour le PFPDT urgemment amélioré, particuliè- rement eu égard à la sensibilité des données stockées sur ces PC.

L’accès physique aux PC „biométrique“ et du secrétariat n’est pas réglé de manière assez claire. Pour les deux postes, il faut par conséquent établir une liste définissant clairement les ayants droit, le nom- bre de ces derniers devant par ailleurs être réduit à un minimum. La même remarque est valable pour les droits d’accès logique aux données de ces ordinateurs (comptes d’utilisateur), ainsi que pour l’accès physique et logique aux sauvegardes des données.

Le PFPDT considère en outre problématique le fait que la transmission de données personnelles bio- métriques a lieu par WiFi, protocole qui n’offre pas les mêmes standards de sécurité qu’une transmis- sion par câble, surtout que ce réseau WiFi peut également être utilisé par les membres pour un accès privé à Internet. Il propose par conséquent que la liaison entre le PC „biométrique“ et le PC du secré- tariat, de même que la liaison entre ce dernier et le modem/routeur ADSL, soient établies par câble et que le réseau WiFi ne soit à l’avenir plus qu’utilisé pour permettre aux membres d’accéder à Internet. La transmission des données personnelles (biométriques) aura ainsi lieu de manière plus sûre et sé- parée du trafic Internet occasionné par les membres.

E. 5.9

Droit d’accès

E. 5.9.1

Point de départ

Selon l’art. 8 LPD, toute personne peut demander au maître du fichier si des données la concernant sont traitées.

Chez le CT XX, les membres peuvent s’adresser à tout moment au président, pour obtenir un droit de regard sur leur gabarit biométrique. Le président s’est engagé à étendre ce droit d’accès à l’ensemble des données traitées sur les membres.

E. 5.9.2

Jugement du point de vue du PFPDT

Avec l’extension du droit d’accès à toutes les données sur les membres, les droits correspondants des membres seront garantis. Le PFPDT n’a pas d’autres remarques à ce sujet.

6. Résultats

Sur la base de l’analyse des documents qui nous ont été remis et du contrôle effectué le 11.02.2010 selon l’art. 29 LPD, le PFPDT parvient à un jugement global critique du système biométrique de réser- vation. Le contrôle de protection des données a révélé que le traitement de données personnelles effectué par le CT XX depuis l’introduction du système biométrique de réservation n’a pas lieu de ma- nière entièrement conforme aux exigences de protection des données. Lors de son contrôle, le

PFPDT est tombé sur des états de fait qui nécessitent une amélioration ou une modification du point de vue de la protection des données.

Partant de ce constat global, le PFPDT arrête son jugement global à l’attention du CT XX sous la forme de :

■ Constatations et/ou ■ Recommandations au sens de l’art. 29 al. 3 LPD.

E. 6.1

Données biométriques en tant que données personnelles

Avec des données biométriques d’empreintes digitales, il s’agit de données personnelles selon l’art. 3 lit. a LPD. Des données biométriques sous forme brute ou dérivée (gabarit) rendent une personne identifiable. Leur collecte laisse en général – en particulier celle d’empreintes digitales – des traces. La collecte de données biométriques brutes (ou dérivées) est ainsi susceptible de produire un profil de mouvements de la personne concernée. De ce fait, il existe lors de la collecte de données biométri- ques pour la personne concernée un grand potentiel d’atteintes à la personnalité.

E. 6.2

But du traitement de données

Chaque traitement de données personnelles peut entraîner une atteinte au droit à la protection de la sphère privée selon l’art. 13 al. 2 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.; RS 101). Un tel traitement nécessite par conséquent un motif justificatif particulier. Des considérations pratiques ou une simple convivialité pour les clients ne représentent pas un motif justi- ficatif suffisant pour le traitement de données biométriques.

Selon les indications du CT XX, la saisie des données biométriques vise exclusivement la lutte auto- matique contre les abus de réservation et d’utilisation des courts de tennis. L’avantage pour le CT XX résiderait dans le fait qu’aucune vérification personnelle de

l’identité des joueurs ne doit être effectuée (par exemple par l’exploitation d’une réception) lors de la réservation et l’utilisation des courts. Le nouveau système biométrique de réservation remplace l’ancien système basé sur un NPI, avec lequel de nombreux cas d’abus auraient été constatés. Selon les indication du CT XX, le nombre de mem- bres a fortement augmenté depuis l’introduction du nouveau système, tandis que les courts ont été moins utilisés durant la même période, ce qui serait en rapport avec l’absence de possibilités d’abus. L’avantage pour les membres réside dans le fait qu’ils ne doivent pas être porteurs d’une carte de membre. Les réservations depuis Internet restent en outre possibles, comme avec le système précé- dent.

Le nouveau système biométrique de réservation du CT XX poursuit des buts plausibles. Le PFPDT aimerait cependant exprimer ses sérieuses préoccupations quant à la question de savoir s’il n’existe pas d’autres alternatives pour éviter les mêmes abus, mais qui seraient moins attentatoires aux droits de la personnalité des personnes concernées (cf. à cet égard aussi le résultat de la vérification de proportionnalité au chiffre 6.5.1.1, Recommandation 2).

E. 6.3

Licéité du traitement de données / Consentement des per- sonnes concernées

Le traitement de données biométriques requiert un motif justificatif (art. 12 et 13 LPD). Dans le cas présent, le consentement de la personne concernée entre en ligne de compte. Le système biométri- que de réservation a été introduit suite à une décision correspondante d’une AG. Une alternative va- lable a été offerte aux membres qui n’étaient pas d’accord avec le système, de sorte que qu’on peut partir de l’idée que les membres qui utilisent le système biométrique ont donné leur consentement.

Du point de vue du PFPDT, il manque cependant d’importantes informations, comme en particulier les modalités de traitement, l’indication explicite de l’existence d’une alternative sans exploitation de don- nées biométriques et le fait que le nom de famille des membres du club peut être publié dans le sys- tème de réservation (voir plus loin 6.5.1.2).

Recommandation 1 :

a) Le CT XX doit établir d’ici au 31.12.2010 une feuille d’information expliquant les modalités de traitement des don- nées biométriques, la possibilité d’une alternative sans exploita- tion de données biométriques, ainsi que le fait que le nom de fa- mille des membres est publié dans le système de réservation, à moins que l’option de pseudonymisation n’ait été choisie. Les points principaux du traitement de données doivent être décrits, par exemple le détail de l’utilisation des gabarits biométriques, le lieu de stockage des données, le moment de leur destruction, la journalisation des transactions, les différentes personnes ayant accès aux données et les éventuels destinataires de données.

b) Cette feuille d’information doit en outre être signée par la direc- tion du CT XX et dotée d’un contrôle de versions.

c) Cette feuille d’information doit enfin être remise immédiatement à tous les membres existants et automatiquement à tous les nou- veaux arrivants avant leur enrôlement. Le CT XX doit bien enten- du veiller à ce que chaque nouveau membre dispose d’un temps suffisant pour prendre connaissance de ce document avant son inscription.

E. 6.4

Traitement selon la bonne foi / Transparence

L’enrôlement n’est possible qu’avec le concours du membre. Sans sa participation, aucune donnée biométrique ne peut être collectée par le CT XX. Le traitement de données a lieu pour ce point de manière transparente et est reconnaissable par la personne concernée.

21/27

On doit néanmoins regretter que l’information des membres quant aux modalités de traitement des données soit insuffisante. Les membres ont certes été informés à l’occasion de l’AG oralement par le président du club, puis au moyen de la notice d’utilisation du système. Pour un traitement de données aussi transparent que possible, il faudrait remettre une feuille d’information, en plus des explications orales du président du club et de la notice d’utilisation informant purement sur la manipulation correcte du système. Cette feuille d’information doit décrire au minimum ce qui passe avec les données per- sonnelles et qu’une alternative sans collecte de données biométriques existe (cf. Recommandation 1).

E. 6.5

Proportionnalité du traitement de données

E. 6.5.1

Proportionnalité matérielle

E. 6.5.1.1

Centralisation des données biométriques

La mise en œuvre de processus biométriques dans le domaine privé représente en fonction de leur conception dans le cas concret d’espèce une atteinte plus ou moins intensive aux droits de la person- nalité des personnes concernées. Avant la mise en œuvre de tels processus biométriques, il faut donc en principe toujours vérifier si d’autres mesures appropriées, mais moins attentatoires aux droits fon- damentaux des personnes concernées, ne permettraient pas également d’atteindre le but visé. Par ailleurs, il faut déjà lors du choix et de la conception du processus biométrique veiller à choisir un sys- tème qui soit le plus économique possible en données et qui reste dans un rapport raisonnable avec le but visé.

Dans le cas présent, il s’agit d’un système de réservation pour des courts de tennis. La biométrie est mise en œuvre pour la vérification des membres du club. On n’atteint une économicité de données qu’en collectant les données biométriques absolument nécessaires à la vérification.

Pour la mise en œuvre du nouveau système de réservation, des gabarits sont générés à partir des empreintes digitales des membres, puis stockés dans une base de données centrale. Les données brutes, c’est-à-dire les images originales des empreintes digitales, ne sont pas conservées. La limita- tion de n’enregistrer que les gabarits biométriques, comme cela est effectué par le CT XX, est donc proportionnelle du point de vue de l’économicité de données.

Les données biométriques sont liées de manière permanente aux personnes et susceptibles de pro- duire un profil de mouvements de la personne concernée. Précisément lorsqu’il s’agit de domaines aussi sensibles que les empreintes digitales, ces données biométriques devraient de ce fait être mé- morisées dans le domaine d’influence de la personne concernée

respectivement de l’utilisateur. Le principe de la proportionnalité matérielle exige que pour les systèmes biométriques capables de fonc- tionner également sans centralisation des données, les caractéristiques biométriques ne soient dans la mesure du possible pas sauvegardées dans une base de données centrale, mais bien plutôt sur un support exclusivement accessible au seul utilisateur.

De ce qui a été dit jusqu’à présent, il découle qu’il existe les trois variantes suivantes pour une réalisa- tion du système conforme à la protection des données dans le cadre de la mise en œuvre de la bio- métrie pour vérifier les personnes autorisées à accéder à une installation de loisirs. Pour des caracté- ristiques laissant des traces (physiques ou numériques) comme les empreintes digitales ou les photo- graphies du visage, seules les variantes a) et b) avec cartes individuelles garantissent un niveau de

protection suffisant. La variante c) sans carte est par contre envisageable pour des caractéristiques biométriques ne laissant pas de trace comme le réseau veineux du doigt ou le contour de la main.

a) Décentralisation : (sur cartes)

Comme le PFPDT le stipule dans son guide concernant les systèmes de reconnaissance biométrique datant de septembre 2009, la protection de la personnalité des personnes concernées est au mieux assurée lors de la mise en œuvre de la biométrie dans le domaine privé, si

1. les données biométriques sont conservées sous forme de gabarits chiffrés sur un support sé- curisé se trouvant sous contrôle individuel de la personne concernée ; et 2. la personne concernée doit libérer explicitement et consciemment chaque accès aux don- nées ; et 3. la vérification de l’identité n’a lieu que sur le support sécurisé, de telle sorte que les données biométriques ne quittent à aucun moment l’environnement sécurisé du support et le contrôle de la personne concernée (comparaison biométrique sur carte, cf. guide p. 13).

b) Pseudodécentralisation : (avec cartes)

Un niveau approximativement aussi élevé quant à la protection de la personnalité peut être atteint au moyen d’une pseudodécentralisation. Cette solution a aussi été esquissée par le Tribunal administratif fédéral dans son jugement du 4 août 2009 (A-3908/2008) concernant le cas KSS. À la différence de la vraie décentralisation, les données biométriques sont certes mémorisées de manière centralisée, mais un accès logique à ces données n’est possible qu’à l’aide d’un code de correspondance mémo- risé sur une carte possédée exclusivement par la personne concernée. Cela signifie en détail ce qui suit :

1. les données biométriques sont conservées de manière centralisée sous forme de gabarits chiffrés (et non de données brutes comme une image ou une photographie) ; 2. les gabarits biométriques sont conservés de telle sorte qu’aucun lien avec une personne iden- tifiée ou identifiable ne puisse être établi par le maître de fichier. Des données statistiques ou accessoires peuvent leur être associées, pour autant quelles ne soient pas identifiantes ; 3. le lien entre un gabarit biométrique et la personne concernée est établi uniquement avec l’autorisation expresse et libre de cette dernière lorsqu’elle fait usage de sa carte individuelle .

c) Centralisation : (sans carte)

Dans le cas où l'introduction de cartes individuelles n'est pas souhaitée dans le cadre d'une vérifica- tion biométrique des membres d'un club de loisirs, seule un système avec une centralisation des réfé- rences biométriques est envisageable. Comme de tels systèmes sont théoriquement appropriés pour accomplir une identification biométrique, ils doivent respecter l'ensemble des conditions suivan- tes pour ne pas être jugés disproportionnés pour effectuer une pure vérification biométrique :

1. seules des caractéristiques biométriques sans trace (physique ou numérique) peuvent être exploitées ; 2. les données biométriques sont conservées de manière centralisée sous forme de gabarits chiffrés (et non de données brutes comme une image ou une photographie) ; 3. les gabarits biométriques sont conservés de telle sorte qu'aucun lien avec d'autres données identifiantes de personnes concernées ne puisse être établi par le maître de fichier. Des don-

nées statistiques (ex : sexe) ou accessoires (ex : date d'expiration) peuvent cependant leur être associées, pour autant qu'elles ne soient pas identifiantes ; 4. le lien entre un gabarit biométrique et la personne concernée est établi de manière volatile par le système de reconnaissance, uniquement pour attester de son appartenance aux membres. La suite des opérations (confirmation de réservation…) a lieu sur une base non biométrique.

Recommandation 2 :

a) À l'avenir, mais au plus tard le 30.06.2011, le CT XX renonce à l'actuelle mémorisation centralisée de gabarits biomé- triques d'empreintes digitales. b) Si le CT XX souhaite maintenir l'utilisation de données biomé- triques pour la vérification des membres dans le système de réservation, alors il faut que : - les données biométriques, y compris celles qui ont déjà été enregistrées centralement, soient mémorisées sur un support restant dans la sphère d'utilisation et sous contrôle de la per- sonne concernée (solution minimale de « comparaison biomé- trique sur carte », cf. p. 13 du guide) ; ou - les données biométriques soient centralisées sous forme de gabarits chiffrés, toutefois sans aucun lien avec d'autres don- nées personnelles, de telle sorte qu'une correspondance avec une personne identifiée ou identifiable ne soit possible qu'avec l'autorisation explicite et consciente de la personne concernée par l'usage de sa carte individuelle ; ou - seules des caractéristiques biométriques ne laissant aucune trace (physique ou numérique) soient exploitées, pour autant que les données soient mémorisées sous forme de gabarits biométriques chiffrés, sans aucune correspondance perma- nente avec d'autres données identifiantes de personnes concernées.

E. 6.5.1.2

Publication des données de réservation sur Internet

Une publication de données personnelles sur Internet est toujours liée à des risques particuliers. De ce fait, le but de la publication doit être au préalable soigneusement examiné et la publication doit être limitée aux seules données absolument nécessaires pour atteindre ce but. À chaque fois que possi- ble, l'accès doit par exemple être restreint par mot de passe aux seules personnes qui en ont vraiment besoin pour atteindre le but visé.

Dans le cas présent, la publication sur Internet sert à permettre aux membres du club d'effectuer une réservation en ligne. Cette finalité peut être atteinte sans restrictions, si l'accès est limité aux seuls membres du club. La réalisation technique de cette limitation d'accès ne devrait poser que peu de problèmes, car l'activation d'une réservation requiert maintenant déjà une connexion. La limitation peut certainement être atteinte au moyen

d’une identification d’utilisateur avec authentification par mot

de passe. Un protocole chiffré et éprouvé comme SSL (Secure Socket Layer) permet aujourd’hui d’assurer la confidentialité des transmissions de données. La longueur des clés doit alors s’élever au moins à 128 bit.

Recommandation 3 :

iÛ~ÅÅ≠ë=~ì=ëóëí≠ãÉ=ÇÉ=ê¨ëÉêî~íáçå=Éå=äáÖåÉ=Ççáí=ÆíêÉ=éêçí¨Ö¨=
é~ê=ãçí=ÇÉ=é~ëëÉ=Éí=é~ê=íê~åëãáëëáçå=ÅÜáÑÑê¨É=E¨í~í=~ÅíìÉä=ÇÉ=
ä~=íÉÅÜåáèìÉF=~ìñ=ëÉìäë=ãÉãÄêÉë=Çì=ÅäìÄ=ÇÛáÅá=~ì=PNKNOKOMNMK

Pour la réservation en ligne, la nomination des personnes n’est en outre pas indispensable. Il suffit de pouvoir reconnaître si un court est libre ou occupé. La plus-value de pouvoir trouver un partenaire de jeu par son vrai nom doit avoir lieu sur une base volontaire. Si le véritable nom est cependant celui qui est affiché par défaut, il y a le risque que beaucoup de membres laissent apparaître ce nom par mé- connaissance ou confort, sans qu’ils soient véritablement d’accord avec la publication de leur nom dans le système de réservation. C’est la raison pour laquelle les membres doivent être rendus atten- tifs à ce fait et surtout à la possibilité de pseudonymisation (cf. à cet égard la recommandation 1a).

E. 6.5.2

Proportionnalité temporelle

À l’heure actuelle, le CT XX n’effectue aucune destruction régulière de données. Les données du sys- tème de réservation sont effacées tous les 2-3 ans pour des raisons de place, les autres données ne sont jusqu’à présent jamais effacées. Aucun délai de destruction n’est prescrit nulle part. La propor- tionnalité temporelle n’est donc pas satisfaite.

Recommandation 4 :

iÉ=`q=uu=Ççáí=áåíêçÇìáêÉ=ÇÉë=Ç¨ä~áë=ÇÉ=ÇÉëíêìÅíáçå=éçìê=íçìíÉë=
äÉë=Ççåå¨Éë=ëìê=äÉë=ãÉãÄêÉëI=ó=Åçãéêáë=ÅÉääÉ=ÉåêÉÖáëíê¨Éë=ëìê=ÇÉë=
ëìéézêíë=ÇÉ=ë~ìîÉÖ~êÇÉ=EÄ~ÅâìéFK=È=ÅÉí=ÉÑÑÉíI=áä=ëçìãÉí=~ì=mcmaq=
ìåÉ=éêçéçëáíáçå=ÇÉ=ê≠ÖäÉãÉåí=ÇÉë=Ç¨ä~áë=ÇÉ=ÇÉëíêìÅíáçå=ÇÉë=ÇçåJ
å¨Éë=Éí=ÉåíêÉéêÉåÇ=äÉë=~Ç~éí~íáçåë=íÉÅÜåáèìÉë=å¨ÅÉëë~áêÉë=éçìê=
ãÉííêÉ=Éå=ÌìîêÉ=ÅÉ=ê≠ÖäÉãÉåí=~î~åí=äÉ=PNKNOKOMNMK=

E. 6.6

Finalité du traitement

De par la centralisation actuellement pratiquée des gabarits biométriques, on ne peut pas totalement exclure un détournement de la finalité (i.e. un traitement dépassant l’empêchement des abus) de ces données délicates. Un détournement de finalité par liaison avec d’autres fichiers ou par communica- tion à un tiers externe serait possible. Comme une modification du but du traitement des données biométriques centralisées n’est pas contrôlable par les personnes concernées, il faut privilégier des

solutions techniques permettant de garantir au mieux le respect de la finalité. Du point de vue du res- pect de la finalité, il faut prévoir la mémorisation décentralisée des données

biométriques sur un sup- port se trouvant dans la sphère d’utilisation de la personne concernée. On peut ici se référer à la re- commandation 2.

E. 6.7

Exactitude des données (fiabilité, applicabilité)

Pour des raisons de protection des données, le taux FAR devrait être minimisé, sans pour autant trop péjorer le taux FRR. Un seuil d’acceptation optimal doit en outre être choisi. Chaque système biomé- trique présente un certain taux (non nul) de FAR. La vérification ne peut de ce fait avoir lieu de ma- nière entièrement fiable.

Pour les personnes dont certaines caractéristiques biométriques manquent ou ne sont que difficile- ment lisibles (jeunesse/vieillesse, cicatrices, etc.), il faut planifier et mettre en œuvre une applicabilité équivalente du système de reconnaissance.

Le nombre des minuties par gabarit utilisées par le CT XX se trouve dans la fourchette de tolérance. Les personnes qui ne peuvent pas utiliser pour cause de caractéristiques manquantes ou de qualité insuffisante pour le système ont la possibilité d’effectuer leur réservation au moyen d’un NPI et jouis- sent ainsi d’une alternative équivalente. Le PFPDT n’a pas de remarques au sujet de l’exactitude des données, à part le fait qu’il est d’avis que la centralisation des données n’est pas proportionnelle et par conséquent qu’une décentralisation des données sur un support restant dans la sphère d’utilisation de la personne concernée s’impose (cf. recommandation 2).

E. 6.8

Sécurité des données

La sécurité des données chez le CT XX n’est pas suffisamment garantie, précisément eu égard à la sensibilité des données personnelles utilisées. Les ordinateurs doivent être mieux sécurisés physi- quement, afin de minimiser la probabilité d’un vol. Les droits d’accès physique et logique doivent en outre être mieux réglés et également réduits en nombre, toujours afin de limiter les risques. Une trans- formation du réseau devrait enfin améliorer la sécurité des transmissions de données.

Recommandation 5 :

^Ñáå=ÇÛ~ã¨äáçêÉê=ä~=ë¨Åìêáí¨=~ÅíìÉääÉãÉåí=áåèìÑÑáë~åíÉ=ÇÉë=Ççåå¨ÉëI=
Éå=é~êíáÅìäáÉê=Éì=¨Ö~êÇ=¶=äÉìê=ëÉåëáÄáäáí¨I=äÉ=`q=uu=~=àìëèìÛ~ì=
PNKNOKOMNM=éçìê=W= = ~=
~ã¨äáçêÉê=ä~=ë¨Åìêáí¨=éÜóëáèìÉ=Çì=m`=■ÄáçãÄíêáèìÉ“=Éí=Çì=m`=Çì=
ëÉÅê¨í~êá~í=é~ê=ÇÉë=ãÉëìêÉë=~éêêçéêá¨ÉëK=

ÄK= ê¨ÖäÉãÉåíÉ==äÉë=Çêçáíë=ÇÛ~ÅÅ≠ë=éÜóëáèìÉ=~ì=m`=■ÄáçãÄíêáèìÉ“=Éí=
~ì=m`=Çì=ëÉÅê¨í~êá~íI=Éå=ê¨Çìáë~åí=äÉ=åçãÄêÉ=ÇÛ~ó~åíë=Çêçáí=¶=ìå=
ëíêáÅí=ãáåáãìãK=

ÅK= ê¨ÖäÉãÉåíÉê=äÉë=Çêçáíë=ÇÛ~ÅÅ≠ë=äçÖáèìÉ=¶=íçìíÉë=äÉë=Ççåå¨Éë=
éÉêëçååÉääÉë=ÉåêÉÖáëíê¨Éë=Eë~ìîÉÖ~êÇÉë=Åçãéêáëíëë=FI=Éå=ê¨Çìáë~åí=äÉ=
åçãÄêÉ=ÇÛ~ó~åíë=Çêçáí=¶=ìå=ëíêáÅí=ãáåáãìãK==

ÇK= êÉãáëä~ÅÉê=ä~=íê~åëãáëëáçå=ÇÉ=Ççåå¨Éë=ë~åë=Ñáä=ÉåíêÉ=äÉ=m`=■ÄáçJ
ã¨íêáèìÉ“=Éí=äÉ=m`=Çì=ëÉÅê¨í~êá~íI=~áåëá=èìÉ=ÅÉääÉ=¨îÉåíìÉääÉ=ÉåíêÉ=äÉ=

m`=Çì=ëÉÅê¨í~êá~í=Éí=äÉ=ãçÇÉãLêçìíÉìê=^apiI=é~ê=ìåÉ=äá~áëçå=ÅßJ Ää¨ÉK

E. 6.9

Droit d’accès

Les membres ont en tout temps la possibilité de consulter leurs données personnelles et de les faire actualiser si nécessaire. Le droit d’accès des membres étant garanti, le PFPDT n’a pas de remarques à ce sujet.

7. Conclusions

E. 7.1

Concernant le contrôle de la collecte de données biométri- ques

Dans le but d’endiguer les abus de réservation et d’utilisation des courts de tennis, le CT XX a intro- duit durant l’été 2009 un nouveau système de réservation, collectant et mémorisant des gabarits bio- métriques d’empreintes digitales, en plus des renseignements usuels sur les membres.

Le contrôle de protection des données effectué a fourni au PFPDT un aperçu détaillé du nouveau système biométrique de réservation. La documentation mise à disposition par le CT XX a permis au PFPDT d’examiner les traitements de données correspondants quant au respect des dispositions de protection des données.

Le PFPDT arrive à un jugement global critique de ce système biométrique de réservation. Le contrôle de protection des données a montré que le traitement de données personnelles effectué par le CT XX depuis l’introduction du nouveau système biométrique de réservation n’est pas en tout point conforme aux exigences de protection des données. Le PFPDT a expliqué avec justification, tout ce qui devait être modifié ou amélioré.

E. 7.2

Procédure et prochaines étapes

Le présent rapport de contrôle comprend une série de constatations et de recommandations formu- lées par le PFPDT sur la base des conclusions de l’audit effectué. Le rapport complet de contrôle sera remis au CT XX pour prise de connaissance. Dans un délai de 30 jours après réception, le CT XX devra communiquer au PFPDT s’il a des remarques à formuler et, s’il accepte les recommanda- tions, la proposition de règlement de délais de destruction (cf. recommandation 4). Au cas où le

CT XX refuserait ou ne suivrait pas les recommandations, le PFPDT peut porter l’affaire devant le Tribunal administratif fédéral pour décision (art. 29 al. 4 LPD).

En considération de la sensibilité des données personnelles traitées et des réactions de certains membres du club, le contrôle du nouveau système du CT XX quant au respect des exigences de pro- tection des données s’est avéré très utile. Les constatations et recommandations faites par le PFPDT montrent la direction à suivre par d’autres exploitants privés de systèmes biométriques dans le do- maine des clubs de loisirs.

Pour les raisons susmentionnées, il existe un intérêt fondamental à sensibiliser le public à ce genre de collecte de données et à l’informer en particulier sur le contrôle de protection des données effectué chez le CT XX et sur les résultats obtenus. Se basant sur l’art. 30 al.2

LPD, le PFPDT va donc ren- dre public sur son site (www.edoeb.admin.ch) et sous une forme adaptée et anonymisée le présent rapport de contrôle concernant la collecte de données biométriques dans le cadre de la réservation de courts du club de tennis du CT XX. Il va de soi que cette publication n'aura lieu que sous réserve que du point de vue du CT XX (avec l'accord du fournisseur du système), aucune donnée confidentielle qui pourrait révéler des secrets d'affaire ou influencer la capacité concurrentielle ne sera communiquée. Le CT XX est prié de vérifier que le rapport de contrôle ne contient pas de tels contenus confi- dentiels et de confirmer cet état de fait par écrit au PFPDT dans un délai de 30 jours.

Nous vous prions de prendre bonne note de ce qui précède et vous remercions encore de votre bonne collaboration durant l'établissement des faits.

Berne, le 13 septembre 2010

Préposé fédéral à la protection des données et à la transparence

Hanspeter Thür

E. 8

5. Jugement du point de vue de la protection des données

E. 18

6. Résultats

E. 20

3/27

E. 26

4/27

1. Point de départ

Le club de tennis XX a introduit en été 2009 un nouveau système pour la réservation des courts de tennis. Les empreintes digitales des membres sont dès lors saisies et enregistrées sous forme de gabarits biométriques. Chaque réservation d'un court de tennis doit désormais être confirmée par le numéro de membre et surtout par l'apposition de l'empreinte digitale, afin de pouvoir jouer sur le court correspondant.

Le nouveau système de réservation vise à garantir que seules les personnes autorisées puissent utili- ser les courts du CT XX.

2. Portée du contrôle

Le contrôle de protection des données portait sur les flux de données en rapport avec le nouveau système de réservation. Le point principal résidait dans le traitement des données biométriques col- lectées, ainsi que des données personnelles publiées dans le cadre de la réservation en ligne.

3. Chronologie du contrôle

Début octobre 2009 Le PFPDT apprend l'existence du système biométrique de réservation par le biais de demandes de membres du club. Suite au développement d'une certaine résistance au sein du club et au nombre important (plus de 1000) de personnes concernées, le PFPDT décide de procéder à un établissement des faits. 15.10.2009 Le PFPDT informe le

CT XX par écrit sur le contrôle de protection des données envisagé pour le système de réservation et sur l’établissement des faits prévu sur place. En outre, le PFPDT demande une documen- tation au sujet du nouveau système et des réponses à un formulaire de questions annexées. 30.10.2009 Le CT XX répond au formulaire de questions et envoie une première documentation. 03.12.2009 Le PFPDT pose quelques questions complémentaires. 14.12.2009 Le CT XX répond à ces nouvelles questions et envoie d’autres docu- ments. 14.01.2010 Le PFPDT propose des dates de visite et demande quelles seront les personnes présentes. 27.01.2010 Le rendez-vous est fixé au 11.02.2010. 11.02.2010 Établissement des faits en présence des personnes responsables. fin février 2010 Échange de courriels entre le PFPDT et le CT XX au sujet de questions complémentaires. 05.03.2010 Le PFPDT envoie un factsheet au CT XX en les priant de vérifier maté- riellement le texte et de répondre aux questions supplémentaires. 22.03.2010 Le CT XX confirme par écrit l’exactiture du contenu du factsheet. Avril 2010 Analyse et synthèse de tous les documents et états de fait, ainsi que préparation du rapport final par le PFPDT. 13.09.2010 Envoi au CT XX du rapport final de contrôle du PFPDT.

4. Établissement des faits du 11 février 2010