Avis de contrôle préalable du CEPD sur «*le test de dépistage de stress basé sur la variabilité de fréquence cardiaque (Évaluation du mode de vie)*» au sein du Comité des régions.

Bruxelles, le 17 décembre 2015 (dossier 2015-0509)

1. Procédure

Le 11 juin 2015, le Contrôleur européen de la protection des données («le CEPD») a reçu une notification pour un contrôle préalable conformément à l'article 27, paragraphe 2, point a), du règlement 45/2001 («le règlement») du délégué à la protection des données («DPD») du Comité des régions («CdR»). La notification concerne un nouveau traitement lié à la mesure et à l'évaluation du niveau de stress des membres du personnel, sur la base de la variabilité de leur fréquence cardiaque et de leurs habitudes quotidiennes.

Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans un délai de deux mois, c'est-à-dire au plus tard le 17 décembre 2015, en prenant en compte les suspensions pour les demandes d'informations complémentaires[1].

2. Faits

Finalité et personnes concernées

Dans le cadre de la politique du CdR pour la prévention du stress et de l'épuisement, son service médical envisage de proposer à son personnel la possibilité de se soumettre à une évaluation de mesure de niveau de stress réalisée par un contractant externe. Ce test fournira au personnel un rapport d'évaluation sur la manière de mieux gérer les facteurs de stress et les risques psychosociaux sur le lieu de travail. Les membres du personnel peuvent participer à ce programme de manière volontaire.

Base juridique et licéité

- Les articles 3 et 8 du décret royal belge du 10 avril 2014 concernant la prévention des risques psychologiques au travail obligent l'employeur à analyser et à cartographier les risques psychologiques éventuels au travail;
- La participation au test est volontaire conformément à l'article 5, point d), du règlement.

Procédure et données traitées

Le CdR négociera un contrat de prestation de services d'une durée d'un an avec un contractant finnois (Firstbeat). Un projet de contrat a été envoyé au CEPD ainsi que d'autres documents connexes.

Le projet de contrat prévoit que «*les données à caractère personnel peuvent être traitées à titre individuel ou collectivement avec les fichiers de données à caractère personnel de Firstbeat et de ses filiales. Tout transfert de données à caractère personnel en dehors de ces sociétés est soumis au consentement distinct de la personne concernée… Les données à caractère personnel peuvent être*

[1] L'affaire a été suspendue dans l'attente d'informations complémentaires du 16 juin 2015 au 26 juin 2015, du 23 juillet 2015 au 29 septembre 2015 et le 20 novembre 2015 respectivement, et pour commentaires du DPD et du responsable du traitement du 3 décembre 2015 au 10 décembre 2015.

traitées par Firstbeat, son sous-traitant ou un prestataire de services tiers (qui a obtenu auprès de Firstbeat le droit d'utiliser le Service et de proposer le Service à ses clients en tant que prestataire de services) par un spécialiste bien-être («wellness specialist») tiers agréé conformément à la Loi finnoise sur la protection des données. Ce spécialiste bien-être tiers agréé est autorisé à utiliser le Service de manière indépendante, comme convenu avec Firstbeat.» Le «*spécialiste bien-être tiers agréé*» mentionné est l'infirmière du CdR. Il est également indiqué que les données à caractère personnel seront «*utilisées de manière anonyme à des fins statistiques et de recherche marketing*».

Les participants ont un premier contact avec l'infirmière du service médical du CdR qui attachera un appareil de mesure avec des électrodes sur leur poitrine pour mesurer leur fréquence cardiaque. Ils peuvent ensuite se connecter à un serveur en ligne, choisir une langue et cliquer sur «démarrer» en fournissant les informations suivantes: prénom, nom de famille, date de naissance, genre, taille, poids, catégorie professionnelle, estimation d'activité aérobique, traitement médicamenteux à long terme et maladies de longue durée, dix questions liées à l'activité physique, habitudes alimentaires, consommation d'alcool, stress, niveau d'énergie, suffisance du sommeil, etc. Les participants doivent alors fixer la date et l'heure à laquelle ils ont commencé leurs mesures. Par ailleurs, ils ont l'opportunité de remplir un journal avec des informations pour les jours de mesures et toutes informations complémentaires, telles que les moments reposants ou stressants, ou les sessions d'exercice, pour tirer le meilleur parti de l'évaluation. Les participants ont le choix de communiquer à Firstbeat leur adresse et leur numéro de téléphone ou toutes autres informations via le serveur en ligne.

Le port de l'appareil et la fourniture en ligne d'informations pertinentes au serveur doivent au minimum durer trois jours et trois nuits.

À l'expiration de la période de mesure, les participants retournent l'appareil de mesure à l'infirmière du CdR. Elle connectera l'appareil au serveur Firstbeat et téléchargera les mesures. Un rapport d'évaluation sera communiqué aux participants à ce moment. Les participants peuvent accéder à leur rapport en se connectant au compte individuel qu'ils ont initialement créé lorsqu'ils ont commencé les mesures.

L'infirmière du CdR sera formée par le contractant externe pour pouvoir expliquer aux participants les résultats de leur rapport d'évaluation et leur montrer comment améliorer leur vie quotidienne.

Droit à l'information

Les participants seront informés par le biais d'un «*avis juridique concernant le traitement des données au titre du test "Évaluation du mode de vie"»* (avis de confidentialité). Ce document sera publié sur l'intranet du service médical et les participants en recevront un exemplaire lors de la remise de l'appareil de mesure de la fréquence cardiaque.

Droits d'accès et de rectification

La notification indique que les participants peuvent exercer leur droit d'accès et de rectification en envoyant un courriel au service médical du CdR. Ils peuvent corriger toute donnée à caractère personnel inexacte ou incomplète dans leur dossier médical. Ils peuvent demander à ce que leur rapport d'évaluation soit retiré de leur dossier médical.

Toutefois, le CdR, en réponse aux questions du CEPD, a indiqué que ceci n'est plus pertinent dans la mesure où le service médical du CdR ne conservera pas le rapport d'évaluation, mais uniquement la liste des noms des participants.

Politique de conservation

Le service médical du CdR proposera à Firstbeat d'adopter une période de conservation de deux ans, de sorte que si les participants décident de refaire le test pendant ce délai, ils puissent être en mesure de comparer les résultats.

Les données anonymes seront utilisées à des fins statistiques et de recherche marketing. Ceci signifie que les noms, les adresses électroniques et les informations du groupe permettant d'identifier une personne seront supprimés du serveur de Firstbeat. Firstbeat conservera les relevés de rythme cardiaque avec l'âge et le sexe.

Conservation et mesures de sécurité

Le service médical ne conservera aucun fichier papier ou électronique. Le rapport d'évaluation sera directement communiqué au participant.

Concernant le point de savoir si une évaluation concernant le risque lié à la sécurité des informations a été réalisée sur la sous-traitance du traitement à Firstbeat, le CdR a répondu qu'aucune évaluation de ce genre n'avait été réalisée, dans la mesure où Firstbeat est une société finnoise réputée dont les serveurs sont situés en Finlande.

3. Aspects juridiques

3.1. Contrôle préalable

Le traitement de données à caractère personnel examiné est effectué par une institution de l'UE, le CdR. Par ailleurs, le traitement est à la fois manuel – ce qui fait partie ou ce qui est destiné à faire partie d'un système de classement (rapport d'évaluation imprimé) – et automatique (informations fournies par les participants via le serveur en ligne de l'outil d'évaluation de Firstbeat et production du rapport d'évaluation). Le règlement est donc applicable.

Le traitement implique le traitement de données se rapportant à la santé, telles que les relevés de rythme cardiaque, les maladies chroniques, les traitements médicamenteux et les habitudes alimentaires. Le traitement vise à évaluer le niveau de stress des participants et de leur assurer un coaching par l'infirmière du CdR sur la manière de mieux gérer leur vie quotidienne. En raison du caractère sensible des données traitées, le traitement est susceptible de présenter des risques particuliers au regard des droits et des libertés des participants et il est donc soumis au contrôle préalable du CEPD[2].

Le CEPD déterminera ci-dessous les pratiques du CdR qui ne semblent pas conformes aux principes du règlement et adressera au CdR les recommandations appropriées.

3.2. Consentement

Le traitement analysé est basé sur la participation volontaire des membres du personnel du CdR. Le CEPD rappelle au CdR que dans une situation d'emploi, le consentement est une question sensible dans la mesure où il n'est pas certain que ce consentement soit librement donné. Il est par conséquent important que le CdR veille à ce que chaque participant donne son consentement «sans ambiguïté» avant de participer au test, comme requis par l'article 5, point d), du règlement. Ceci signifie que le consentement des participants doit être librement donné, spécifique et informé, et les participants indiquent par là qu'ils acceptent que leurs données soient collectées pendant toutes les différentes étapes du traitement[3]. Le CdR doit donc informer de manière adéquate tous les participants que leur participation et la collecte de leurs données se font sur la base du volontariat [article 11, paragraphe 1, point d), du règlement] et qu'ils peuvent retirer leur consentement à tout moment.

3.3. Concept du responsable du traitement et du sous-traitant et article 23 du règlement

Comme expliqué ci-avant, le CdR signera un contrat avec Firstbeat, un contractant externe finnois, en vue de mesurer et évaluer le niveau de stress sur la base de la variabilité de la fréquence cardiaque des participants et de leurs habitudes quotidiennes.

---

[2] L'article 27, paragraphe 2, du règlement dresse une liste des traitements qui sont susceptibles de présenter des risques au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités, y compris, au point a), les traitements de données relatives à la santé.

[3] L'article 2, paragraphe h), du règlement indique que le consentement de la personne concernée signifie «*toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*».

À la lumière de l'article 23 du règlement, Firstbeat agira pour le compte du CdR et, par conséquent, doit être considéré comme le sous-traitant, alors que le CdR est le responsable du traitement. Ceci signifie que CdR est l'institution communautaire chargée de déterminer les finalités et les moyens du traitement [article 2, paragraphe d), du règlement] et Firstbeat ne doit procéder au traitement que sur instructions du CdR [article 23, paragraphe 2, point a)].

En particulier, le CdR, en tant que responsable du traitement (article 4, paragraphe 2, du règlement), doit indiquer dans le projet de contrat les conditions suivantes:

i) Firstbeat ne doit traiter que des données adéquates, pertinentes et non excessives, et les données traitées (relevés du rythme cardiaque, informations communiquées par les participants et rapport d'évaluation) ne doivent être traitées que pour la finalité pour laquelle elles sont collectées;

ii) Firstbeat ne sera pas autorisé à transférer des informations traitées ou à externaliser un service à un sous-traitant ou à un prestataire de services tiers, sauf accord du CdR;

iii) Firstbeat ne doit pas non plus traiter des données à d'autres fins incompatibles (c'est-à-dire transférer les données à d'autres sociétés à des fins de marketing) ;

iv) Firstbeat doit mettre en œuvre la période de conservation des données demandée par le CdR, et

v) Si un participant souhaite avoir accès à ses données brutes traitées par Firstbeat, ce dernier doit être en mesure de garantir ce droit.

Concernant les obligations de Firstbeat en matière de confidentialité, de protection des données et de mesures de sécurité conformément à l'article 23, paragraphe 2, point d), du règlement, le CdR doit veiller à ce que des dispositions spécifiques soient ajoutées au projet de contrat concernant ces obligations. Concernant les obligations de confidentialité et de sécurité, compte tenu que le sous-traitant est une société de droit finnois, elle doit en principe être soumise à l'article 16 et à l'article 17, paragraphe 3, deuxième tiret, de la directive 95/46/CE, transposée dans la loi finnoise relative à la protection des données (voir ci-après au point 3.7).

3.4. Droit d'accès et de rectification

À la lumière de l'article 4, paragraphe 1, point d), du règlement, le CdR doit veiller à ce que les données des participants soient exactes et mises à jour; il doit donc prendre toutes les mesures raisonnables pour garantir que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement soient effacées ou rectifiées. Ceci signifie qu'il incombe au CdR de garantir que les participants soient en mesure d'exercer leur droit d'accès (article 13 du règlement) et de rectification (article 14 du règlement).

Le CEPD note que l'infirmière du CdR discutera avec chaque participant du rapport d'évaluation et lui montrera comment gérer le stress et améliorer sa vie quotidienne. Les participants peuvent également refaire le test et être en mesure de comparer les résultats. Le CdR ne souhaite pas conserver une copie du rapport d'évaluation. Toutefois, dans l'éventualité où un participant demande la conservation d'une copie du rapport et des notes connexes éventuelles dans son dossier médical, le CdR doit être en mesure de satisfaire cette demande. Les participants doivent être alors en mesure d'exercer leur droit d'accès à leur rapport d'évaluation à tout moment et leur droit de rectification/de mise à jour s'ils souhaitent refaire le test.

Par ailleurs, le CEPD souligne que dans l'éventualité où un participant demande à accéder à ses données brutes (informations traitées par Firstbeat), le CdR doit veiller à ce que Firstbeat soit en mesure de garantir ce droit.

Le CdR doit effacer les informations inexactes figurant dans la notification et clairement préciser les recommandations qui précèdent à la fois dans la notification et dans le projet de contrat.

3.5. Conservation des données

L'article 4, paragraphe 1, point e), du règlement dispose, à titre de principe général, que les données à caractère personnel ne doivent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement.

Le CEPD note que Firstbeat consentira à effacer les données traitées sur demande du CdR. Si le CdR envisage de conclure un contrat d'une année avec Firstbeat, la période de conservation de deux ans prévue par le CdR semble excessive par rapport à la finalité du traitement. Le CEPD recommande au CdR de fixer une période de conservation nécessaire et raisonnable n'excédant pas la durée du contrat avec Firstbeat et de veiller à ce que le sous-traitant mette en œuvre cette période de conservation. Par ailleurs, le CdR doit explicitement stipuler dans le projet de contrat que Firstbeat doit adopter des garanties adéquates pour s'assurer que ces données ne soient pas traitées à d'autres fins, ou utilisées à l'appui de mesures ou de décisions concernant un participant en particulier. La notification devrait être mise à jour en conséquence.

À la lumière du paragraphe 3.1, le CdR doit également adopter une période de conservation du rapport d'évaluation et des notes éventuelles de l'infirmière, si un participant demande à ce que ces informations soient conservées dans son dossier médical.

Conformément aux informations communiquées, les données «anonymisées» seront utilisées par Firstbeat à des fins statistiques et de recherche marketing. Même si les noms, adresses électroniques et informations relatives au groupe sont supprimés, le risque de ré-identifier ces données sensibles est très élevé[4]. Les données confiées à Firstbeat doivent être considérées comme des données à caractère personnel même si les informations qui précèdent sont effacées. Le CEPD recommande ainsi au CdR d'insérer une stipulation dans le projet de contrat soulignant le caractère sensible des données et le risque élevé de ré-identification. Par conséquent, Firstbeat ne doit pas traiter les données sur ses serveurs, qu'elles soient rendues anonymes ou non, à des fins statistiques ou de marketing.

Si le CdR ne souhaite utiliser des données anonymes qu'à des fins statistiques, le CEPD recommande que les données rendues anonymes ne soient pas publiées sur l'internet et qu'elles ne soient utilisées qu'à des fins de bonne gestion de l'institution et dans l'intérêt des membres de son personnel.

3.6. Informations à fournir aux participants

Les articles 11 et 12 du règlement concernent les informations à fournir aux personnes concernées afin d'assurer un traitement loyal et transparent de leurs données à caractère personnel. En l'espèce, certaines des données sont collectées directement auprès des participants et d'autres informations auprès d'autres entités (à savoir le rapport d'évaluation auprès de Firstbeat et l'évaluation des résultats et le coaching par l'infirmière). Par conséquent, les deux articles s'appliquent.

Quant au contenu de l'avis de confidentialité, le CdR doit
i) clarifier le rôle du CdR et de Firstbeat, dans la mesure où il n'existe aucune référence à ce dernier dans l'avis de confidentialité;

ii) mentionner la possibilité pour les participants d'exercer leur droit d'accès et de rectification de leur rapport d'évaluation et des notes connexes ainsi que des données brutes (informations traitées par Firstbeat), comme expliqué au point 3.3; et

[4] Voir l'avis 05/2014 du Groupe de travail Article 29 sur les techniques d'anonymisation adopté le 10 avril 2014
(http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp2l 6_en.pdf)

iii) indiquer la période de conservation des données conservées par le service médical du CdR et par Firstbeat.

Le CdR doit inclure toutes les recommandations qui précèdent dans l'avis de confidentialité et publier la version mise à jour sur l'intranet avant de lancer le traitement.

3.7. Sécurité

Même si le CdR ne traite directement aucune donnée à caractère personnel, il est tenu par l'article 23 du règlement: *«Lorsque le traitement est effectué pour son compte, le responsable du traitement choisit un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation prévues par l'article 22 et veille au respect de ces mesures».* À cette fin, le CdR doit obtenir une garantie formelle (une attestation de sécurité) que Firstbeat respecte effectivement les obligations qui lui incombent en matière de confidentialité et de sécurité des données à caractère personnel qui lui sont confiées.

4. Conclusion

En conclusion, rien ne porte à croire que les dispositions du règlement sont violées, pour autant que les recommandations formulées ci-après soient pleinement prises en considération. Le CdR devrait notamment:

- clarifier dans le projet de contrat avec Firstbeat les rôles du responsable du traitement et du sous-traitant et indiquer dans le projet de contrat toutes les conditions telles qu'expliquées au point 3.3;

- supprimer les informations inexactes figurant dans la notification et indiquer que les participants peuvent exercer leur droit d'accès et de rectification du rapport d'évaluation et des autres notes connexes, ainsi que des données brutes (point 3.4);

- fixer une période de conservation spécifique pour les données collectées pour Firstbeat et pour le CdR (point 3.5);

- inclure toutes les informations figurant au point 3.6 dans l'avis de confidentialité et publier une version mise à jour sur l'intranet du CdR avant de lancer le traitement;

- obtenir une garantie formelle (c'est-à-dire une attestation de garantie) de Firstbeat que les informations qui lui sont confiées seront conservées conformément aux conditions de confidentialité et de sécurité figurant dans le règlement (point 3.7).

Dans le cadre de la procédure de suivi, veuillez envoyer au CEPD une version modifiée de la notification, de l'avis de confidentialité, du projet de contrat et de la garantie de Firstbeat, dans un délai de trois mois et avant de lancer le traitement, pour démontrer que les recommandations du CEPD qui précèdent ont été mises en œuvre.

Fait à Bruxelles, le 17 décembre 2015

(signé)
Wojciech Rafal WIEWIOROWSKI