Politique d'Intersurgical sur le Traitement des Données Personnelles

Introduction

Intersurgical est amenée à traiter des données personnelles relatives à ses employés, sous-traitants, visiteurs, clients et prospects dans le cadre de son activité. Intersurgical prendra toutes les mesures raisonnables pour le faire conformément à cette politique.

Dispositions générales

1. Le but de ce document est de définir les procédures selon lesquelles Intersurgical Ltd (ci-après dénommé Intersurgical) collecte, utilise, divulgue et/ou traite les données personnelles conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE Règlement Général sur la Protection des Données (ci-après dénommé RGPD). Il explique également comment il garantit le niveau adéquat de protection des données prescrit par d'autres lois nationales du Royaume-Uni relatives à la protection des données.
2. Le traitement des données personnelles doit répondre aux exigences du RGPD et être conforme aux lois nationales applicables en matière de confidentialité.
3. Les autres termes et définitions utilisés dans la présente Politique ont la même signification que dans le RGPD et les lois nationales applicables en matière de confidentialité.

Informations sur le(s) responsable(s) du traitement et le(s) sous-traitant(s) des données

4. Intersurgical est le principal responsable du traitement et sous-traitant des données personnelles détenues et traitées :
   - 4.1. Intersurgical Ltd, identifiant d'entité juridique 1488409, adresse – Crane House, Molly Millars Lane, Wokingham, Berkshire, United Kingdom, RG41 2RZ
5. Les sous-traitants sont également d'autres sociétés du groupe Intersurgical.
6. Des informations sur le responsable du traitement et le sous-traitant par différentes catégories de données personnelles sont fournies à l'annexe 1.

Responsabilité et obligations du responsable du traitement et du sous-traitant

7. Droits du responsable du traitement :
   - 7.1. procéder, réviser et mettre à jour cette procédure et d'autres documents internes liés au traitement des données personnelles ;
   - 7.2. prendre des décisions concernant la divulgation de données personnelles ;
   - 7.3. approuver et désigner une personne ou un service approprié pour protéger les droits des personnes concernées ;
   - 7.4. sous-traiter le traitement des données personnelles ou partager des données personnelles avec des tiers.
8. Responsabilités du responsable du traitement des données :
   - 8.1. garantir que la protection des données personnelles est conforme au RGPD et aux lois nationales applicables en matière de confidentialité ;
   - 8.2. de s'assurer que le traitement répond aux exigences de cette procédure et garantit la protection des droits de la Personne Concernée ;
   - 8.3. mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer la protection des données personnelles ;
   - 8.4. désigner le sous-traitant qui peut prendre les mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de cette procédure et garantisse la protection des droits de la personne concernée. Le traitement par le sous-traitant est régi par un contrat ;
   - 8.5. informer l'autorité de contrôle compétente du traitement des données personnelles conformément au RGPD et aux lois nationales applicables en matière de confidentialité.
9. Devoirs du responsable du traitement :
   - 9.1. définir la finalité pour laquelle les données sont traitées ;
   - 9.2. organiser la mise en place de systèmes de surveillance ou d'autres systèmes nécessaires au traitement des données personnelles ;
   - 9.3. fournir les droits d'accès et l'autorisation pour le traitement des données personnelles ;
   - 9.4. analyser les problèmes technologiques, méthodologiques et organisationnels liés au traitement des données personnelles et intégrer de manière efficace les garanties nécessaires dans le traitement afin de répondre aux exigences de cette procédure et de protéger les droits des personnes concernées ;
   - 9.5. aider les employés et fournir des recommandations relatives au traitement des données personnelles au sous-traitant ;
   - 9.6. s'assurer que tous les employés impliqués dans le traitement des données connaissent l'état actuel de la législation en matière de traitement des données personnelles ;
   - 9.7. autres mesures prises pour garantir que les responsabilités et devoirs du contrôleur de données sont remplis.

Traduction du Document Original

Données personnelles

10. Les données personnelles couvrent toute information relative à une personne vivante (personne concernée) qui peut être identifiée à partir de ces informations. Le traitement désigne toute utilisation faite des données, y compris leur collecte, leur stockage, leur modification, leur divulgation ou leur destruction.

Base et finalités du traitement des données personnelles

11. Les actions suivantes sont prises lors du traitement des données personnelles : Intersurgical a identifié que les données personnelles sont traitées par les éléments suivants :
    - 11.1. le système de vidéosurveillance est utilisé pour surveiller ou enregistrer les activités qui peuvent assurer la protection des actifs de l'entreprise, la qualité des processus de production et les procédures légales en matière de sécurité du travail ;
    - 11.2. l'entreprise est administrée en interne tout en gérant les dossiers des ressources humaines, en administrant les commandes des clients et en poursuivant les ventes.
12. Des informations détaillées sur la base juridique et les finalités du traitement des données personnelles par différentes catégories de données personnelles sont fournies à l'annexe 2.
13. Le système de vidéosurveillance est utilisé et couvre les installations intérieures et extérieures (périmètre extérieur et territoire de l'installation, parkings et entrées des locaux, entrepôts et locaux des bâtiments de fabrication, lieux de travail communs dans les locaux industriels) d'Intersurgical. Le traitement des données de vidéosurveillance est défini en détail dans le manuel des employés (Royaume-Uni).

Principes de protection des données

14. Intersurgical traite les données personnelles conformément aux principes de protection des données suivants :
    - 14.1. La Société traite les données personnelles de manière licite, équitable et transparente.
    - 14.2. La Société collecte des données personnelles uniquement pour des finalités déterminées, explicites et légitimes.
    - 14.3. La Société traite les données personnelles uniquement lorsqu'elles sont adéquates, pertinentes et limitées à ce qui est nécessaire aux finalités du traitement.
    - 14.4. La Société conserve des données personnelles exactes et prend toutes les mesures raisonnables pour garantir que les données personnelles inexactes soient rectifiées ou supprimées sans délai.
    - 14.5. La Société conserve les données personnelles uniquement pendant la durée nécessaire au traitement.
    - 14.6. La Société adopte des mesures appropriées pour garantir que les données personnelles sont sécurisées et protégées contre tout traitement non autorisé ou illégal, ainsi que contre toute perte, destruction ou dommage accidentels.

Transferts de données personnelles et destinataires des données

15. Intersurgical ne transfère pas de données personnelles à des tiers. Les autres sociétés du groupe Intersurgical ne sont pas considérées comme des tiers.
16. Tout transfert de données personnelles doit être conforme au RGPD et aux lois nationales applicables en matière de confidentialité.
17. Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou du sous-traitant, qui a accès aux données personnelles, ne doivent pas traiter ces données sauf sur instructions du responsable du traitement, sauf si le droit de l'Union européenne ou d'un État membre l'y oblige.

Contrôles techniques et organisationnels

Intersurgical a mis en place les contrôles suivants pour garantir la protection des données personnelles :

18. Des mesures techniques et organisationnelles appropriées sont prises contre le traitement non autorisé ou illégal des données personnelles et contre la perte, la destruction ou l'endommagement accidentels des données personnelles :
    - 18.1. garantir l'existence d'une protection, d'un processus et d'un contrôle d'accès aux données personnelles ;
    - 18.2. chaque utilisateur doit utiliser un compte disposant des autorisations appropriées au travail qu'il effectue à ce moment-là ;
    - 18.3. les utilisateurs autorisés ne peuvent effectuer que certaines procédures ou actions avec des données personnelles pour lesquelles ils disposent d'une autorisation ;
    - 18.4. l'accès aux données personnelles doit être protégé par des mots de passe ou d'autres moyens de sécurité. Si les mots de passe sont utilisés, ils doivent respecter les exigences suivantes :
        - 18.4.1. doivent être émis, mis à jour et protégés pour garantir la confidentialité ;
        - 18.4.2. doivent comporter au moins 8 caractères et comporter une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux du clavier comme l'astérisque ou les symboles monétaires, à l'exclusion de toute information personnelle ;
        - 18.4.3. les mots de passe sont changés régulièrement (au moins une fois tous les 6 mois) ;
        - 18.4.4. doivent être modifiés après la première connexion.
    - 18.5. les données personnelles sont protégées contre tout accès non autorisé aux communications électroniques ;
    - 18.6. l'accès à tous les centres de données et salles de serveurs utilisés pour héberger le matériel et les logiciels sur lesquels les données personnelles sont stockées est limité uniquement aux membres du personnel autorisés à y travailler ;
    - 18.7. le matériel sur lequel les données personnelles sont stockées est protégé par un logiciel antivirus et dispose de correctifs de sécurité du système d'exploitation à jour ;

Traduction du document original

19. Procédure d'octroi, d'annulation et de modification des droits d'accès des utilisateurs au traitement des données d'image :
    19.1. les droits d'accès des utilisateurs sont accordés, annulés ou modifiés avec l'accord du supérieur direct du salarié sur la base de procédures internes ;
    19.2. les droits d'accès des utilisateurs aux actifs informationnels doivent être supprimés à la fin de leur emploi, contrat ou accord, ou ajustés en cas de changement. En cas de résiliation, les droits d'accès d'un individu aux informations et aux actifs associés aux installations et services de traitement de données sont immédiatement supprimés ou suspendus.
20. Les durées de conservation des différentes catégories de données personnelles sont définies par le service responsable d'Intersurgical et fournies à l'annexe 3.
21. Afin de garantir l'accès aux données personnelles pendant la période de conservation, les données sont sauvegardées conformément au calendrier. Le support de stockage est stocké dans un environnement sécurisé avec un journal des accès conservé. L'accès est réservé au personnel autorisé.

Gestion des failles de sécurité des données personnelles

22. Si un membre du personnel ayant des droits d'accès aux données personnelles a remarqué une violation de la sécurité des informations/données (toute divulgation involontaire/à dessein d'informations/ données confidentielles ou personnelles à des personnes non autorisées, soit par la divulgation accidentelle, la perte ou le vol des informations/ données), ils doivent immédiatement en rendre compte au délégué à la protection des données ou à leur responsable direct.
23. Les violations de données personnelles sont gérées conformément au plan de gestion des violations de données personnelles.
24. En évaluant le risque découlant de la violation de la sécurité dans différentes situations, le délégué à la protection des données examine quelles seraient les conséquences néfastes potentielles pour les individus. En outre, le degré d'impact, de dommage et de conséquences de la violation est pris en considération, ce qui conduit à des décisions sur les mesures à prendre pour contenir la violation.

Droits de la personne concernée

25. Les droits de la Personne concernée (individu) sont les suivants :
    25.1. connaître (être informée) du traitement de ses données personnelles ;
    25.2. avoir accès à ses données personnelles ;
    25.3. s'opposer au traitement de ses données ;
    25.4. demander la rectification de ses données personnelles ;
    25.5. demander l'effacement de ses données personnelles ;
    25.6. restreindre le traitement ultérieur des données personnelles, à l'exception du stockage, lorsque les données traitées enfreignent les dispositions du RGPD ou les lois nationales applicables en matière de confidentialité ;
    25.7. recevoir les données personnelles la concernant, qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine.
26. Les règles générales de mise en œuvre des droits de la personne concernée sont les suivantes :
    26.1. La personne concernée doit envoyer sa demande par écrit au responsable du traitement ou au sous-traitant. Le formulaire électronique de l'entreprise peut être utilisé pour effectuer cette demande.
    26.2. une personne peut être tenue de fournir une pièce d'identité ou de vérifier son identité conformément aux lois applicables, ou par des moyens de communication électroniques, qui permettent une identification fiable de la personne, pour vérifier son identité.
    26.3. si la demande de la personne concernée est reçue par courrier ou par coursier, une copie notariée du document d'identité signé par un notaire doit être présente. Si la personne concernée est représentée par une autre personne, la procuration générale doit être fournie comme preuve de l'autorisation du représentant à agir au nom de la personne concernée. De plus, la copie notariée de la pièce d'identité du représentant signée par un notaire doit être présente.
    26.4. la personne concernée reçoit des informations ou des données personnelles demandées après réception de la demande concernant le traitement des données personnelles et après que la vérification de l'identité de la personne concernée soit terminée ;
    26.5. répondre à la demande de la personne concernée dans les 30 jours calendaires suivant l'introduction de la demande ;
    26.6. si la demande de la personne concernée a été reçue sous forme écrite, la réponse doit être rédigée sous la même forme.
27. Une Personne concernée a le droit d'accéder à ses données personnelles et cette demande est traitée en conséquence :
    27.1. Une personne a le droit d'accéder à ses données personnelles traitées par l'entreprise et d'obtenir des informations sur les sources et le type de données personnelles qui ont été collectées, la finalité du traitement et les destinataires des données auxquels les données sont divulguées ou ont été divulgués au cours de l'année dernière ; le droit à la vie privée des tiers doit être garanti lors de l'exercice du droit de la personne concernée d'accéder à ses données personnelles, par exemple lorsque la personne concernée a connaissance des données vidéo et que des tiers peuvent être identifiés ou que d'autres informations peuvent violer leur vie privée (par exemple, le numéro d'immatriculation du véhicule), la vidéo doit être retouchée ou éliminée d'une autre manière, supprimant ainsi la possibilité d'identifier des tiers ;
    27.2. en général, les demandes d'accès d'une personne concernée concernant le traitement de ses données personnelles doivent recevoir une réponse dans un délai de 30 jours calendaires à compter de la date de réception d'une demande complète. Lorsque la

Traduction du document original

demande de la personne concernée est soumise par écrit, la réponse du responsable du traitement ou du sous-traitant doit également être exécutée par écrit. Lorsque la personne concernée fait la demande par des moyens électroniques, et sauf demande contraire de la personne concernée, les informations sont fournies sous une forme électronique couramment utilisée.

27.3. Le responsable du traitement ou le sous-traitant fournira gratuitement une copie des données personnelles en cours de traitement une fois par an. Pour toute copie supplémentaire demandée par la personne concernée, le responsable du traitement ou le sous-traitant peut facturer des frais raisonnables basés sur les coûts administratifs déterminés par l'autorité de contrôle compétente.

28. La Personne concernée a le droit de s'opposer au traitement des données personnelles et la procédure se déroule en conséquence :
    28.1. la Personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, au traitement des données personnelles la concernant ;
    28.2. la personne concernée a le droit de s'opposer au traitement des informations personnelles avant qu'elles ne soient traitées pour les motifs de l'article 21 du RGPD ou des lois nationales applicables en matière de confidentialité. La personne concernée sera informée par écrit de nos intentions de traiter ces données (collecte, utilisation, divulgation par transmission, etc.) avant leur traitement avec la possibilité de refuser, d'une explication des procédures juridiques qui doivent être suivies lors du traitement par courrier ou par voie électronique, et la détermination d'un délai raisonnable dans lequel la personne concernée a le droit d'exprimer sa volonté ;
    28.3. lorsque l'opposition de la personne concernée est légalement justifiée, le responsable du traitement et le sous-traitant doivent suspendre le traitement de ces données personnelles, sans délai et sans frais, et en informer dûment les destinataires des données ;
29. La personne concernée a le droit de demander l'effacement ou la limitation du traitement des données personnelles (cela ne s'applique pas au stockage des données personnelles) :
    29.1. si la personne concernée se rend compte que ses données personnelles sont traitées illégalement et non conforme aux procédures, elle ou son représentant doit en informer le responsable du traitement. Les mesures supplémentaires suivantes doivent être prises : le responsable du traitement doit vérifier gratuitement la légitimité et l'intégrité du traitement des données, des mesures immédiates pour supprimer les données personnelles non autorisées et générées frauduleusement doivent être mises en œuvre et le traitement de ces données doit être suspendu, à l'exception du stockage des données;
    29.2. le responsable du traitement et le sous-traitant peuvent conserver les données personnelles pendant la suspension des opérations de traitement ou jusqu'à leur destruction (à la demande de la personne concernée ou après l'expiration de la durée de conservation des données). D'autres actions liées aux données personnelles ne peuvent être effectuées que :
        29.2.1. à des fins d'enquête sur les circonstances de la suspension du traitement des données ;
        29.2.2. si la personne concernée donne son consentement à la poursuite du traitement ;
        29.2.3. pour protéger les droits et les intérêts des tiers.
    29.3. le responsable du traitement doit immédiatement, au plus tard dans les 30 jours, informer la personne concernée ou son représentant des mesures prises en rapport avec la demande reçue ;
    29.4. les données personnelles de la personne concernée sont détruites ou le traitement est suspendu à la demande de la personne concernée ou de son représentant autorisé conformément à l'identification de la personne concernée ;
    29.5. le responsable du traitement informe immédiatement, au plus tard dans les 30 jours, les destinataires des données de la demande de la personne concernée ou de son représentant concernant les données personnelles et de la mise en œuvre de la suspension du processus de données personnelles. La suspension du traitement des données personnelles n'est pas appliquée si elle est impossible en raison d'un nombre énorme de personnes concernées, d'une période de données ou de dépenses excessives. Dans ce cas, l'autorité de contrôle compétente doit être immédiatement informée.
30. Le droit de rectification est mis en œuvre en conséquence :
    30.1. Afin de garantir que les données personnelles de la personne concernée sont inexactes ou incomplètes, le responsable du traitement peut demander à la personne concernée de fournir des preuves à l'appui ;
    30.2. si les données personnelles de la personne concernée (telles que corrigées à la demande de la personne concernée) ont été transmises aux destinataires des données, le responsable du traitement en informera les destinataires, à moins que cela ne soit impossible ou n'exige un effort disproportionné. La personne concernée a le droit de demander des informations sur ces destinataires.
31. Le droit de recevoir les données personnelles relatives à la personne concernée, qu'elle a soumises au responsable du traitement dans un format systématique, couramment utilisé et lisible par ordinateur, n'est mis en œuvre que si les données sont traitées par des moyens automatisés sur la base d'un consentement ou d'un contrat.
32. Le responsable du traitement a le droit de refuser de mettre en œuvre les droits de la personne concernée uniquement sur la base des exigences du RGPD ou des lois nationales applicables.

Traduction du document original

Responsabilités individuelles

33. Les individus sont responsables d'aider l'entreprise à maintenir leurs données personnelles à jour. Les individus doivent informer l'organisation si les données fournies à l'organisation changent, par exemple si une personne déménage ou modifie ses coordonnées bancaires.
34. Les individus peuvent avoir accès aux données personnelles d'autres individus et de nos clients dans le cadre de leur emploi. Lorsque tel est le cas, l'organisation compte sur les individus pour l'aider à remplir ses obligations en matière de protection des données envers le personnel et envers les clients.
35. Les personnes ayant accès aux données personnelles sont tenues :
    - 35.1. d'accéder uniquement aux données auxquelles ils sont autorisés à accéder et uniquement à des fins autorisées ;
    - 35.2. de ne pas divulguer de données sauf à des personnes (que ce soit à l'intérieur ou à l'extérieur de l'organisation) qui disposent d'une autorisation appropriée ;
    - 35.3. d'assurer la sécurité des données (par exemple en respectant les règles d'accès aux locaux, d'accès à l'ordinateur, y compris la protection par mot de passe, et de stockage et de destruction sécurisés des fichiers) ;
    - 35.4. ne pas retirer des locaux de l'organisation les données personnelles, ni les appareils contenant ou pouvant être utilisés pour accéder à des données personnelles, sans adopter des mesures de sécurité appropriées (telles que le cryptage ou la protection par mot de passe) pour sécuriser les données et l'appareil ;
    - 35.5. de ne pas stocker de données personnelles sur des disques locaux ou sur des appareils personnels utilisés à des fins professionnelles ; et
    - 35.6. de signaler immédiatement les violations de données dont ils ont connaissance à [nom de la personne/du délégué à la protection des données].
36. Le non-respect de ces exigences peut constituer une faute disciplinaire, qui sera traitée dans le cadre de la procédure disciplinaire de l'organisation. Des violations importantes ou délibérées de cette politique, telles que l'accès aux données des employés ou des clients sans autorisation ou motif légitime de le faire, peuvent constituer une faute grave et conduire à un licenciement sans préavis.

Provisions finales

37. Tout employé qui traite des données personnelles dans l'exercice de ses fonctions professionnelles doit suivre cette procédure, les exigences relatives au traitement des données personnelles conformément au RGPD et aux lois nationales applicables.
38. Les salariés sont informés de cette procédure en la signant. Le nouvel employé doit être initié à la procédure le premier jour d'embauche.
39. Cette procédure doit être revue au moins une fois par an et, si nécessaire, amendée ou modifiée conformément aux processus internes.

Traduction du document original

Annexe 1 de la Procédure de Traitement des Données Personnelles
Informations sur le(s) responsable(s) du traitement et le(s) sous-traitant(s) des données

No.	Catégorie de données personnelles	Responsable(s) du traitement des données	Processeur(s) de données
1.	Données des employés	Intersurgical Ltd	Intersurgical Ltd
2.	Données des candidats lors des campagnes de recrutement	Intersurgical Ltd	Intersurgical Ltd
3.	Données des participants aux investigations cliniques (pseudonymes, pas de données de catégorie particulière)	Intersurgical Ltd	Intersurgical Ltd
4.	Données client (entité juridique)	Intersurgical Ltd	Intersurgical Ltd
5.	Activités de surveillance post-commercialisation et de suivi clinique post-commercialisation	Intersurgical Ltd	Intersurgical Ltd
6.	Données des clients potentiels (personnes morales)	Intersurgical Ltd	Intersurgical Ltd
7.	Données du prestataire/fournisseur	Intersurgical Ltd	Intersurgical Ltd
8.	Données revendeur/distributeur	Intersurgical Ltd	Intersurgical Ltd
9.	Enregistrements de vidéosurveillance	Intersurgical Ltd	Intersurgical Ltd
10.	Registres de contrôle des entrées	Intersurgical Ltd	Intersurgical Ltd
11.	Informations personnelles/données d'utilisation/ de comportement	Intersurgical Ltd	Intersurgical Ltd

Traduction du document original

Annexe 2 de la Procédure de Traitement des Données Personnelles
Base juridique et finalités du traitement des données personnelles

No.	Catégorie de données personnelles	Base légale	Fins commerciales
1.	Données des employés	Consentement de la personne concernée (article 6, paragraphe 1, point a) du RGPD) Exécution d'un contrat ou requise avant la conclusion d'un contrat (article 6, paragraphe 1, point b) du RGPD) Obligation légale (article 6, paragraphe 1, point c) du RGPD)	Administration interne
2.	Données des candidats lors des campagnes de recrutement	Consentement de la personne concernée (article 6, paragraphe 1, point a) du RGPD) Intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (article 6, paragraphe 1, point f) du RGPD)	Administration interne
3.	Données des participants aux investigations cliniques (pseudonymes, pas de données de catégorie particulière)	Consentement de la personne concernée (article 6, paragraphe 1, point a) du RGPD)	Recherches scientifiques
4.	Données client (entité juridique)	Consentement de la personne concernée (article 6, paragraphe 1, point a)), exécution d'un contrat ou requis avant la conclusion d'un contrat (article 6, paragraphe 1, point b) du RGPD)	Fourniture de services/produits Service client
5.	Activités de surveillance post-commercialisation et de suivi clinique post-commercialisation	Obligation légale (article 6, paragraphe 1, point c) du RGPD)	Qualité et sécurité des produits
6.	Données des clients potentiels (personnes morales)	Consentement de la personne concernée (article 6, paragraphe 1, point a) du RGPD) Exécution d'un contrat ou requise avant la conclusion d'un contrat (article 6, paragraphe 1, point b) du RGPD)	Fourniture de services/produits Marketing direct
7.	Données du prestataire/fournisseur	Exécution d'un contrat ou requise avant la conclusion d'un contrat (article 6, paragraphe 1, point b) du RGPD)	Fourniture de services/produits Service client Administration interne
8.	Données revendeur/distributeur	Exécution d'un contrat ou requise avant la conclusion d'un contrat (article 6, paragraphe 1, point b) du RGPD)	Fourniture de services/produits Service client Administration interne
9.	Enregistrements de vidéosurveillance	Intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (article 6, paragraphe 1, point f) du RGPD)	Protection des biens, fourniture de services/produits (qualité)
10.	Registres de contrôle des entrées	Intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (article 6, paragraphe 1, point f) du RGPD)	Protection des biens, chronométrage des employés
11.	Informations personnelles/données d'utilisation/ de comportement	Consentement de la personne concernée (article 6, paragraphe 1, point a) du RGPD) (informations personnelles) Intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (article 6, paragraphe 1, point f) du RGPD) (données d'utilisation, de comportement)	Il n'y a aucune finalité au traitement de ce type d'informations. Intersurgical n'a pas l'intention de traiter ces données à des fins commerciales, mais elle est consciente que ces informations peuvent être traitées par les employés eux-mêmes sur des ordinateurs et des téléphones portables et par le service informatique d'Intersurgical à des fins de maintenance des équipements.

Traduction du document original

Annexe 3 de la Procédure de Traitement des Données Personnelles
Durées de conservation des données pour différentes catégories de données personnelles

No.	Catégorie de données personnelles	Durée de conservation	Commentaires, base pour cette période
1.	Données des employés	Diverses formes de 1 à 50 ans – confirmations détaillées dans l'avis de confidentialité des employés	Loi sur la protection des données de 1998 ; Calendrier de conservation des Archives nationales : dossiers du personnel des employés
2.	Données des candidats lors des campagnes de recrutement	6 mois à compter de l'exercice de recrutement	En raison des délais imposés à divers actes de discrimination. Les documents des candidats retenus seront dans tous les cas transférés dans le dossier RH.
3.	Données des participants aux investigations cliniques (pseudonymes, pas de données de catégorie particulière)	5 ans après l'investigation clinique	
4.	Données client (entité juridique)	1 à 10 ans après le dernier achat	Loi sur la protection des données de 1998 ; Calendrier de conservation des Archives nationales : documents comptables
5.	Activités de surveillance post-commercialisation et de suivi clinique post-commercialisation	5 ans	Actes juridiques concernant les équipements médicaux
6.	Données des clients potentiels (personnes morales)	2 ans après le dernier contact avec une personne	Besoins de l'entreprise
7.	Données du prestataire/fournisseur	1 à 10 ans après le dernier achat	Loi sur la protection des données de 1998 ; Calendrier de conservation des Archives nationales : documents comptables
8.	Données revendeur/distributeur	1 à 10 ans après le dernier achat	Loi sur la protection des données de 1998 ; Calendrier de conservation des Archives nationales : documents comptables
9.	Enregistrements de vidéosurveillance	30 jours	Intérêt légitime – protection des biens, historique des accidents de sécurité
10.	Registres de contrôle des entrées	1 an	Intérêt légitime – protection des biens, historique des incidents
11.	Informations personnelles/données d'utilisation/ de comportement	1 an	Intérêt légitime – protection des informations confidentielles, enquête sur les incidents de sécurité

Traduction du document original