AVIS DE CONFIDENTIALITÉ RELATIF AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Rapports de vulnérabilité et de sécurité – Articles 13 et, le cas échéant, 14 du règlement (UE) 2016/679

1. Responsable du traitement

Le responsable du traitement est Nice s.p.a, dont le siège social est situé Via Callalta n° 1, Oderzo (TV), Italie, numéro d'identification fiscale/numéro de TVA 03099360269 / 02717060277, adresse PECaccounting@pec.niceforyou.com (le « Responsable du traitement »). Le Responsable fait partie du groupe Nice. En fonction du produit ou du composant concerné, d'autres sociétés du groupe ou des entités juridiques tierces peuvent participer au traitement tel que décrit dans la présente Déclaration de confidentialité.

2. Délégué à la protection des données et coordonnées

Le délégué à la protection des données (« DPO »), lorsqu'il a été désigné, peut être contacté à l'adresseniceprivacy@niceforyou.com ou à l'adresse postale Nice spa, Via Callalta n° 1, Oderzo (TV). Les signalements de vulnérabilités peuvent être envoyés à l'adresse security@niceforyou.com. Cette boîte mail est gérée par du personnel autorisé et les signalements ne sont transmis qu'aux personnes et organisations qui doivent participer à leur évaluation et à leur traitement.

3. Personnes concernées

- les personnes soumettant des rapports de vulnérabilité, d'incident ou autres rapports liés à la sécurité ;
- les personnes de contact, les salariés ou les prestataires de l'organisation au nom de laquelle un rapport est soumis ;
- les utilisateurs, clients ou tiers dont les données figurent dans le rapport, les pièces jointes, les journaux ou les informations fournies ;
- les personnes impliquées dans la gestion technique, organisationnelle ou juridique de l'événement.

Lorsqu'un rapport contient des données relatives à d'autres personnes, l'auteur du rapport ne doit divulguer que les informations strictement nécessaires et, dans la mesure du possible, supprimer ou anonymiser les données non pertinentes.

4. Catégories de données à caractère personnel

- les données d'identification et les coordonnées de l'auteur du signalement et de son organisation ;
- les informations concernant le produit, l'appareil, le logiciel, le micrologiciel, la version ou le composant ;
- le rapport et les communications ultérieures ;

- les données techniques telles que les adresses IP, les identifiants d'appareils, les journaux, les horodatages, les configurations, les résultats de tests, les diagnostics, les captures d'écran, les vidéos, les fichiers et les preuves ;
- les informations contenues dans les systèmes de gestion des tickets, des vulnérabilités ou des incidents ;
- les informations concernant l'impact et l'exploitation éventuelle ;
- les informations figurant dans les communications adressées à l'ENISA, aux CSIRT et aux autorités ;
- les informations relatives à la vérification, à l'atténuation, à la correction, au déploiement des mises à jour et à la clôture ;
- les informations nécessaires pour documenter les décisions, la conformité et la protection juridique.

Le responsable du traitement ne sollicite pas de catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD ni de données relatives aux condamnations pénales et aux infractions. Ces données ne doivent pas être incluses, sauf si c t strictement indispensable. Si elles sont reçues, elles ne seront traitées que lorsque cela est nécessaire et lorsqu'une condition prévue aux articles 9 ou 10 du RGPD et par la législation nationale applicable est remplie, y compris, le cas échéant, pour la constatation, l'exercice ou la défense d'un droit en justice.

5. Finalités et bases juridiques

5.1 Réception, évaluation et traitement des signalements

Les données sont traitées afin de recevoir, d'enregistrer et de vérifier les signalements ; d'identifier le produit, le composant et le propriétaire concernés ; de classer l'incident ; de communiquer avec l'auteur du signalement ; de coordonner l'évaluation, l'atténuation, la correction et la divulgation responsable ; et de prévenir toute utilisation abusive du canal. La base juridique est l'intérêt légitime poursuivi par le responsable du traitement et des tiers à protéger les produits, les réseaux, les systèmes et les utilisateurs, conformément à l'article 6, paragraphe 1, point f), du RGPD. L'article 6, paragraphe 1, point b), du RGPD peut également s'appliquer lorsque le traitement est nécessaire à l'exécution d'un contrat ou à l'exécution de mesures précontractuelles demandées.

5.2 Respect des obligations en matière de cybersécurité

Les données peuvent être traitées afin d'évaluer une vulnérabilité activement exploitée ou un incident grave ; d'émettre des alertes précoces, des notifications, des mises à jour et des rapports finaux ; de se conformer au règlement (UE) 2024/2847 (loi sur la cyber-résilience, « CRA ») et à d'autres dispositions du droit national ou de l'Union ; et de répondre à l'ENISA, aux CSIRT, aux autorités de surveillance du marché, aux autorités chargées de la protection des données ou à d'autres autorités compétentes. La base juridique est le respect d'une obligation légale au titre de l'article 6, paragraphe 1, point c), du RGPD.

5.3 Sécurité et prévention d'autres incidents

Les données peuvent être utilisées pour identifier des vulnérabilités similaires, établir des corrélations entre des événements et des indicateurs techniques, prévenir les attaques ou les accès non autorisés, vérifier les mesures correctives, améliorer la sécurité des produits

et conserver un registre technique. La base juridique est l'intérêt légitime au sens de l'article 6, paragraphe 1, point f), du RGPD.

5.4 Constatation, exercice et défense de droits

Les données peuvent être traitées et conservées afin de documenter les activités et les décisions ; de gérer les réclamations, les inspections et les procédures ; d'établir les responsabilités ; et d'exercer ou de défendre les droits du responsable du traitement, d'autres entités ou de tiers. Les bases juridiques sont l'article 6, paragraphe 1, point f), du RGPD et, le cas échéant, l'article 6, paragraphe 1, point c), du RGPD. Le traitement ne repose pas sur le consentement, sauf indication expresse pour une activité supplémentaire spécifique.

6. Nature de la fourniture

La fourniture de données d'identification est généralement facultative, sauf si l'identification est requise par la loi, la plateforme ou les circonstances. Le signalement anonyme est possible dans la mesure où le canal le permet ; l'absence de coordonnées peut empêcher les clarifications, la vérification, les accusés de réception et les mises à jour. Les informations techniques essentielles doivent être suffisamment complètes, faute de quoi le signalement pourrait ne pas être vérifiable.

7. Traitement et sécurité

Les données sont traitées par voie électronique et, si nécessaire, sous forme documentaire par du personnel autorisé, conformément aux principes de licéité, de loyauté, de transparence, de minimisation, d'exactitude, d'intégrité et de confidentialité. Les mesures de protection adaptées aux risques comprennent des contrôles d'accès, la séparation des tâches, la journalisation, des communications sécurisées, la gestion sécurisée des pièces jointes, le stockage sécurisé des preuves et l'accès limité au strict nécessaire.

8. Divulgation et partage

8.1 Sociétés du groupe et autres entités juridiques

Les données peuvent être partagées avec des sociétés du groupe Nice ou d'autres entités juridiques distinctes agissant en tant que fabricants, importateurs, distributeurs ou mandataires agréés ; responsables du produit, de l'unité commerciale ou du composant ; exerçant des fonctions de R&D, de gestion des produits, de cybersécurité, d'assistance, de qualité, de conformité, de protection de la vie privée ou juridiques ; participant à l'évaluation, à la correction, à la notification ou à la gestion ; ou exposées à la vulnérabilité. En fonction de leur rôle, elles agissent en tant que responsables du traitement indépendants, responsables conjoints du traitement ou sous-traitants dans le cadre des accords requis par le RGPD.

8.2 Prestataires et conseillers

Les destinataires peuvent inclure des prestataires informatiques, de cloud, de messagerie électronique, de gestion des tickets et de cybersécurité ; des laboratoires et des spécialistes techniques ; des conseillers juridiques, des assureurs, des auditeurs et d'autres

professionnels ; des fabricants, des développeurs, des responsables de la maintenance et des fournisseurs de composants. Ils agissent en tant que sous-traitants ou responsables du traitement indépendants selon leur rôle.

8.3 L'ENISA, les CSIRT et les autorités publiques

Lorsque la loi l'exige ou que cela s'avère nécessaire, les données peuvent être communiquées à l'ENISA, notamment par l'intermédiaire de la plateforme unique de signalement de la CRA ; au CSIRT désigné comme coordinateur et à d'autres CSIRT ; aux autorités nationales de surveillance du marché et de cybersécurité ; aux autorités chargées de la protection des données ; aux instances judiciaires, aux forces de l'ordre et à d'autres organismes publics ; aux institutions et organes de l'Union ; ainsi qu'aux autorités publiques du pays du déclarant, du pays où le produit est commercialisé ou utilisé, et d'autres États membres concernés. Les informations peuvent en outre être partagées entre les autorités en vertu du CRA, du droit de l'Union ou du droit national. Les données à caractère personnel communiquées se limitent au strict nécessaire.

9. Transferts internationaux

Le partage entre entités établies dans l'Espace économique européen ne constitue pas un transfert vers un pays tiers au sens du chapitre V du RGPD. Les transferts en dehors de l'EEE s'appuieront, selon le cas, sur une décision d'adéquation, des clauses contractuelles types assorties de mesures complémentaires, des règles d'entreprise contraignantes, une autre garantie reconnue ou, à titre exceptionnel uniquement, une dérogation au titre de l'article 49. Des informations sur les garanties peuvent être demandées au responsable du traitement ou au délégué à la protection des données.

10. Durées de conservation

Les données ne sont pas conservées uniquement pendant la durée nécessaire à l'apport d'une première réponse. Une vulnérabilité ou un incident peut nécessiter des mesures techniques, réglementaires, probatoires et de défense juridique après la clôture de la communication initiale.

Catégorie	Durée normale
Signalements manifestement infondés, spams, doublons sans contenu supplémentaire ou communications non pertinentes	Jusqu'à 12 mois à compter de la classification ou de la clôture, sauf si cela s'avère nécessaire pour prévenir de nouveaux abus.
Signalements techniques évalués mais non confirmés	Jusqu'à 5 ans à compter de la clôture, si nécessaire pour établir des corrélations avec des signalements ultérieurs, documenter les évaluations et prévenir la récidive.
Signalements confirmés, tickets, correspondance, évaluations, décisions, mesures correctives et preuves de clôture	10 ans à compter de la clôture définitive ou de la dernière activité substantielle, si celle-ci est postérieure.

Catégorie	Durée normale
Cas communiqués à l'ENISA, aux CSIRT ou à d'autres autorités	10 ans à compter de la clôture définitive de la procédure ou de la dernière communication avec l'autorité, si celle-ci est postérieure.
Données liées à des litiges, inspections, enquêtes ou procédures	Pendant la durée de la procédure et jusqu'à l'expiration des délais applicables pour l'exercice ou la défense des droits.
Journaux des boîtes mail, des plateformes ou des systèmes de tickets	Normalement 24 mois, sauf s'ils sont liés à un événement ou nécessaires à une enquête.
Données de sauvegarde	Pour le cycle de sauvegarde habituel, à titre indicatif, pas plus de 6 mois, puis écrasement.

Pour les produits encore pris en charge ou susceptibles de produire des effets, les informations techniques et de responsabilité peuvent être conservées jusqu'à la fin de la période de support, puis aussi longtemps que nécessaire pour respecter les obligations légales et protéger les droits. Ces durées peuvent être prolongées lorsque la loi ou une autorité l'exige, pendant des enquêtes ou des litiges, pour des actions en justice ou jusqu'à la résolution définitive. À l'expiration de ces délais, les données sont effacées, anonymisées ou agrégées. Les informations techniques ne se rapportant plus à des personnes physiques peuvent être conservées à des fins statistiques, de recherche et de sécurité. Le responsable du traitement examine périodiquement la nécessité et la proportionnalité de ces conservations.

11. Droits des personnes concernées

Sous réserve du RGPD, les personnes concernées peuvent demander l'accès, la rectification, l'effacement, la limitation du traitement et la portabilité de leurs données, s'opposer à un traitement fondé sur un intérêt légitime et retirer tout consentement. Les demandes peuvent être adressées à niceprivacy@niceforyou.com. L'exercice de ces droits peut être limité ou reporté lorsque la conservation des données est nécessaire pour respecter des obligations légales, assurer la sécurité, protéger les droits de tiers ou pour des actions en justice. Le responsable du traitement peut vérifier l'identité du demandeur.

12. Droit d'opposition

En ce qui concerne le traitement au titre de l'article 6, paragraphe 1, point f), du RGPD, la personne concernée peut s'opposer au traitement pour des motifs liés à sa situation particulière. Le responsable du traitement mettra fin au traitement, sauf s'il existe des motifs impérieux prépondérants ou si le traitement est nécessaire à la défense de droits en justice.

13. Réclamation

Une réclamation peut être déposée auprès de l'autorité de contrôle de l'État membre de résidence habituelle, du lieu de travail ou du lieu où l'infraction présumée a été commise. Pour un responsable du traitement établi en Italie : Garante per la protezione dei dati personali, Piazza Venezia 11, 00187 Rome, Italie, www.garanteprivacy.it. Les voies de recours judiciaires restent ouvertes.

14. Décisions automatisées

Aucune décision n'est prise exclusivement par le biais d'un traitement automatisé produisant des effets juridiques ou des effets tout aussi significatifs. Des outils automatisés peuvent faciliter la classification, la corrélation ou la hiérarchisation, tandis que les décisions importantes restent soumises à un examen humain autorisé.

15. Données obtenues auprès d'autres sources

Les données peuvent provenir des sociétés du Groupe ; des clients, distributeurs, installateurs et partenaires ; des fabricants et fournisseurs ; des chercheurs en sécurité ; de sources publiques ; de plateformes de divulgation de vulnérabilités ; de l'ENISA, des CSIRT et des autorités ; ainsi que des systèmes, produits et infrastructures concernés. Lorsque l'article 14 du RGPD s'applique, la présente notification sera fournie dans les délais applicables, sauf en cas d'exemption.

16. Mises à jour

La présente déclaration de confidentialité peut être mise à jour en fonction des évolutions juridiques, organisationnelles ou techniques. La version en vigueur sera publiée à l'adresse https://www.elero.fr/Avis-de-confidentialite-CRA avec la date de la dernière mise à jour.