ÉTUDE DE CAS CLIENT

DPO EXTERNALISÉ À TEMPS PARTAGÉ POUR UN SERVICE DE SANTÉ AU TRAVAIL INTER-ENTREPRISES (SSTI)

- Audits cybersécurité et RGPD
- Étude et installation d'équipements de sécurité
- Pratiques de développement sécurisé
- Gouvernance de sécurité et de conformité
- ☑ **RSSI et DPO externalisés**
- Formation et sensibilisation

CYBERSECURA
Cybersécurité & Conformité

DPO EXTERNALISÉ POUR UN SERVICE DE SANTÉ AU TRAVAIL - CAS CLIENT

LE CLIENT : PST38

- Service de santé au travail inter-entreprises
- Siège à Grenoble (38)
- Association (100-199 salariés)
- 7 000 entreprises adhérentes représentant près de 83 000 salariés
- Depuis janvier 2021

Le besoin

- La ressource interne alors en charge de la conformité au RGPD a un poste à haute responsabilité dans l'organisation, et ainsi trop peu de temps pour se former et pour gérer cette conformité.
- PST38 devait donc avoir une aide externe pour la mission de DPO qui fonctionne avec une délégation assez forte, pour que les ressources internes puissent se concentrer sur leur coeur de métier.
- Cette prise en charge globale et autonome souhaitée ne pouvait pas être effectuée par le précédent prestataire en charge (cabinet d'avocats).

La solution

- CyberSecura a été désigné auprès de la CNIL comme DPO de PST38.
- Un audit a été effectué pour dresser l'état des lieux de la conformité, permettant de mettre en place un plan d'actions sur plusieurs années pour la montée progressive en conformité globale de l'organisation.
- Travaux pro-actifs et autonomes pour une montée en conformité, incluant la mise en place de toute la documentation de conformité.
- Support réactif mis en place pour toutes les questions des collaborateurs de PST38 et les sollicitations de leurs clients et sous-traitants.

Le(s) résultat(s)

- Progression régulière de la conformité de l'organisation.
- Les collaborateurs de PST38 sont sensibilisés aux enjeux de protection des données personnelles.
- Prise en main complète du besoin, comme souhaité par l'organisation.
- Extension du périmètre d'action souhaité par PST38 suite à une fusion survenue entre plusieurs services de santé au travail.

Intervenants et méthodes

- Juriste en droit du numérique et consultante externe en protection des données.
- Consultant DPO senior spécialisé en données de santé.
- Méthodologie d'état des lieux développée en interne par CyberSecura.
- Méthodologie de montée en conformité développée en interne.
- Mix de sessions en présentiel et de travaux à distance.

FRÉDÉRIQUE GUEDE

Responsable organisation opérationnelle chez PST38

Quels éléments appréciez-vous le plus dans la solution apportée par CyberSecura ?

"L'écoute de Monsieur Rozier, sa disponibilité, et cette prise en charge concrète des choses.
Monsieur Rozier sait nous mettre en confiance, nous écouter pour comprendre notre problématique, la façon dont nous travaillons, quelle est la spécificité de notre service, de façon à nous répondre au mieux et de manière à nous permettre de continuer à travailler efficacement. Car évidemment il faut respecter la loi, mais il faut tout de même continuer à travailler."

Pourquoi avoir choisi CyberSecura ?

"Je ne suis pas sûre que l'offre qui est faite existe chez d'autres prestataires. David prend tout en charge, et c'est extrêmement rassurant. C'est une prise en main complète que je n'ai pas trouvée ailleurs. Depuis que je travaille avec David je me rend compte de l'apport qu'il a."

Le mot de la fin

"Attention, il n'y a pas d'évidences dans le domaine, et il faut vraiment avoir un expert à ses côtés pour pouvoir prendre ces aspects en main efficacement."

DPO EXTERNALISÉ POUR UN SERVICE DE SANTÉ AU TRAVAIL

ENJEUX & CONTEXTE

La conformité au Règlement Général sur la Protection des Données (RGPD) des Services de Santé au Travail Inter-entreprises (SSTI)

Des données personnelles multiples et sensibles

- Un large inventaire de données personnelles : similaire à une entreprise - association avec employés - combinée avec une similitude d'établissement de santé (suivi de la santé des employés d'entreprises adhérentes).
- Les données de santé sont des données sensibles tel que défini par le RGPD, nécessitant une protection renforcée.

Le DPO doit appréhender les traitements de données classiques d'une organisation de type 'association/entreprise' mais aussi les traitements de données particuliers du domaine de la santé.

Diversité d'intervenants et de sites

- Les intervenants des SSTI incluent des intervenants médicaux, para-médicaux, techniques, et administratifs.
- Les SSTI couvrent souvent des zones géographiques étendues, impliquant de nombreux sites pour proposer un service de proximité aux entreprises adhérentes et leurs employés.

Le DPO doit avoir l'agilité nécessaire pour intéragir avec une large diversité d'intervenants, et la capacité à considérer de multiples sites, y compris leurs moyens de communication.

Des ressources rares

- Comme tous les acteurs de santé, les SSTI ne sont pas épargnés par la rareté des intervenants médicaux et des soignants.
- Il est donc critique de permettre aux intervenants des SSTI de se concentrer sur leur coeur de métier.

Le DPO doit pouvoir travailler de manière proactive et avoir une autonomie importante.

LES SSTI EN PLEINE ÉVOLUTION : UN BESOIN DE DPO FIABLES ET AGILES

Des SSTI aux SPSTI

Depuis plusieurs années, la mission des SSTI intègrent la prévention des risques. Les SSTI sont donc devenues de Services de Prévention et de Santé Inter-entreprises - SPSTI. Le nouvel acronyme est peu utilisé mais la réforme était initiée.

Décrets récents

Le décret n° 2022-653 du 25 avril 2022 est un des décrets les plus récents de plusieurs décrets liés à la réforme du domaine, spécifiant les modalités de l'ensemble Socle de Services des SPSTI.

Certification obligatoire

Chaque SPSTi a l'obligation d'obtenir une certification d'ici l'été 2025. L'obtention de cette certification nécessite de pouvoir faire preuve d'une conformité au RGPD de bon niveau.

LES SERVICES DE DPO EN TEMPS PARTAGÉ

Vous accompagner dans votre mise en conformité

Le DPO (i.e. Data Protection Officer, ou Délégué à la Protection des Données personnelles en français) est défini par la CNIL comme étant le "chef d'orchestre" de la conformité en matière de protection des données au sein de l'organisme qui l'a désigné.

Si votre activité nécessite la nomination d'un DPO auprès de la CNIL, si vous traitez des données sensibles au quotidien, et si vous n'avez pas les ressources ou les compétences en interne pour mettre en place un système de gouvernance de la conformité, CyberSecura vous propose ses services de DPO externalisé à temps partagé. Nos consultants en conformité RGPD vous accompagnent dans votre mise en conformité, dans son maintien et dans l'évolution de vos pratiques de gouvernance de votre organisation.

Désigner un DPO est obligatoire pour ...

- Les autorités et organismes publics.
- Les organismes dont le coeur d'activité les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle.
- Les organismes dont le coeur d'activité les amènent à traiter des données dites "sensibles" ou relatives à des condamnations et infractions.

Visibilité sur vos progrès

Une session de reporting structurée est conduite chaque trimestre pour vous offrir cette transparence très appréciée par nos clients.

Interrogez et déléguez

Nous serons votre contact privilégié pour poser vos questions et déléguer vos actions de mise en conformité. Dans le cadre de ses prestations externalisées, CyberSecura émet des préconisations d'expert, mais le client reste toujours libre de prendre les décisions qu'il souhaite.

Les deux grands volets de cette prestation

Un volet de mise en conformité, avec l'écriture de toute la documentation de conformité, les processus d'exercice des droits informatique et libertés, des textes d'informations des personnes concernées, et des textes contractuels obligatoires dans le cadre de la sous-traitance.

Un volet de support, avec une entière disponibilité pour répondre aux questions des collaborateurs de l'entreprise, répondre aux questions des clients/prospects, assurer une réponse adéquate aux demandes d'exercice des droits informatique et libertés, répondre aux questionnements sur la faisabilité d'actions de l'organisation, etc.

Le support est prioritaire, et la documentation quant à elle se fait graduellement.

Cette prestation vous permet de bénéficier d'un macaron destiné à valoriser vos engagements. Ces macarons ont un objectif de communication et vous pourrez les utiliser librement sur tous les supports que vous jugerez pertinents !

Macarons disponibles également en version anglaise

RÉDACTION DE LA DOCUMENTATION DE CONFORMITÉ

Vers une gouvernance de la conformité réglementaire au RGPD

La conformité réglementaire au RGPD nécessite la mise en place et l'élaboration d'une documentation bien spécifique. Cette documentation inclut des éléments ayant pour objectif d'informer vos clients, partenaires et prospects des traitements de données à caractère personnel qui sont réalisés par votre organisation. Mais cette dernière est également indispensable en cas de contrôle de la CNIL et afin de démontrer toute votre pro-activité ainsi que vos efforts de conformité réglementaire.

Dans le cadre d'une prestation de DPO externalisé, nos experts rédigent pour vous

Politique de confidentialité

pour informer les internautes des traitements de données réalisés sur votre site internet.

Clauses de contractualisation des sous-traitants et collaborateurs

afin de contractualiser les obligations réglementaires de vos partenaires et sous-traitants.

Lettre d'engagement de conformité

à destination de vos clients, prospects ou tout autre partenaire qui en ferait la demande.

Mentions d'informations obligatoires

dans vos emailings, mais également sur les formulaires de contact présents sur votre site internet.

Registre des demande d'exercices des droits Informatique et Libertés

afin de répertorier toutes les demandes d'exercice de droits informatique et libertés.

Registre des traitements de données

afin de répertorier tous les traitements de données réalisés par votre organisation.

Analyse d'Impact sur la Protection des Données (AIPD)

afin de construire des traitements de données conformes, éthiques et respectueux de la vie privée.

Etc.

Valorisez vos engagements

Entreprise RGPD Engagé 2023

CYBERSECURA

Macarons disponibles également en version anglaise

CYBERSECURA
Cybersécurité & Conformité

PECB ISO/IEC 27001 LEAD IMPLEMENTER

OFFENSIVE SECURITY OSCP

FRANCE RELANCE

PRESTATAIRE RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

3 Avenue du 8 Mai 1945
38130 Échirolles

06.21.54.42.37

www.cybersecura.com

contact@cybersecura.com