CLIENT CASE STUDY

OUTSOURCED TIME-SHARE DPO FOR AN INTER-COMPANY OCCUPATIONAL HEALTH SERVICE (SSTI)

- Cybersecurity and GDPR audits
- Benchmark and installation of safety equipments
- Secure development practices
- Security and compliance governance
- **Outsourced DPO and CISO**
- Training and awareness

CYBERSECURA
Cybersécurité & Conformité

EXTERNALISED DPO FOR AN OCCUPATIONAL OCCUPATIONAL HEALTH SERVICE - CASE STUDY

THE CLIENT : PST38

- Inter-company occupational health service.
- Head office in Grenoble (38), France.
- Association (100-199 employees).
- 7,000 member companies representing almost 83,000 employees.
- From January 2021.

The need

- The internal resource then in charge of compliance with the GDPR had a position of high responsibility in the organisation, and therefore too little time to train and manage this compliance.
- PST38 therefore needed external help for the DPO mission, which operates with a fairly high level of delegation, so that internal resources could concentrate on their core business.
- The previous service provider in charge (a law firm) was unable to provide the desired comprehensive and autonomous support.

The solution

- CyberSecura has been appointed by the CNIL as PST38's Data Protection Officer.
- An audit was carried out to assess the current state of compliance, enabling an action plan to be put in place over several years to gradually bring the whole organisation into compliance.
- Pro-active and autonomous work to achieve compliance, including the implementation of all compliance documentation.
- Reactive support set up for all questions from PST38 employees and requests from their customers and subcontractors.

The result(s)

- Regular progress in the organisation's compliance.
- PST38 employees are made aware of the challenges of protecting personal data.
- Full control of requirements, as requested by the organisation.
- Extension of the scope of action desired by PST38 following a merger between several occupational health services.

Consultants and methods

- Digital lawyer and external data protection consultant.
- Senior DPO consultant specialising in health data.
- Assessment methodology developed in-house by CyberSecura.
- Methodology for increasing compliance developed in-house.
- Mix of face-to-face sessions and remote work.

FRÉDÉRIQUE GUEDE

Head of Operational Organisation at PST38

What do you appreciate most about the CyberSecura solution?

"Mr Rozier's attentiveness, his availability, and his practical approach to things.
Mr Rozier knows how to put us at ease, how to listen to us to understand our problems, the way we work, the specific nature of our department, so as to provide us with the best possible response and enable us to continue to work effectively. Obviously, we have to comply with the law, but we still have to keep working."

Why did you choose CyberSecura?

"I'm not sure that other service providers offer the same thing. David takes care of everything, and that's extremely reassuring. It's a complete package that I haven't found elsewhere. Since I've been working with David, I've realised just how much he can contribute."

The final word

"Beware, there are no obvious solutions in this field, and you really need to have an expert at your side to be able to deal with these aspects effectively."

Copyright © CyberSecura 2024 - All rights reserved

EXTERNALISED DPO FOR A SERVICE OCCUPATIONAL HEALTH SERVICE

ISSUES & CONTEXT

Inter-company occupational health services (SSTI) compliance with the General Data Protection Regulation (GDPR)

A wide range of sensitive personal data

- A large inventory of personal data: similar to a company - association with employees - combined with a similarity to a healthcare establishment (monitoring the health of employees of member companies).
- Health data is sensitive data as defined by the GDPR, requiring enhanced protection.

The DPO must understand the classic data processing operations of an organisation of the 'association/company' type, but also the specific data processing operations in the health sector.

Diversity of stakeholders and sites

- SSTI staff include medical, paramedical, technical and administrative personnel.
- SSTIs often cover large geographical areas, involving numerous sites in order to offer a local service to member companies and their employees.

The DPO must have the necessary agility to interact with a wide variety of stakeholders, and the ability to consider multiple sites, including their means of communication.

Scarce resources

- Like all healthcare players, SSTIs are not immune to the scarcity of medical and care workers.
- It is therefore vital to enable SSTI staff to concentrate on their core business.

The DPO must be able to work proactively and have considerable autonomy.

SSTIs undergoing major changes: the need for reliable and agile DPOs

From SSTI to SPSTI

For several years now, the mission of SSTIs has included risk prevention. SSTIs have thus become Services de Prévention et de Santé Inter-entreprises - SPSTI. The new acronym is little used, but the reform was initiated.

Recent decrees

Decree no. 2022-653 of 25 April 2022 is one of the most recent of several decrees linked to the reform of the domain, specifying the terms and conditions of the SPSTI Service Base package.

Mandatory certification

Every SPSTi is required to obtain certification by summer 2025. Obtaining this certification requires being able to demonstrate a good level of GDPR compliance.

Copyright © CyberSecura 2024 - All rights reserved

OUTSOURCED TIMSHARE DPO SERVICES

Supporting you in your compliance efforts

The DPO (i.e. Data Protection Officer) is defined by the CNIL as the "conductor" of data protection compliance within the organisation that has appointed him/her.

If your business requires the appointment of a DPO with the CNIL, if you process sensitive data on a daily basis, and if you do not have the resources or skills in-house to set up a compliance governance system, CyberSecura offers you its outsourced DPO services on a time-sharing basis. Our GDPR compliance consultants will support you in achieving and maintaining compliance and in evolving your organisation's governance practices.

Appointing a DPO is mandatory for ...

- Public authorities and bodies.
- Bodies whose core business requires them to carry out regular and systematic monitoring of individuals on a large scale.
- Bodies whose core activity leads them to process so-called "sensitive" data or data relating to convictions and offences

Visibility of your progress

A structured reporting session is conducted on a quarterly basis to provide you with the transparency that is so appreciated by our clients.

Ask and delegate

Your privileged contact to whom you can ask your questions and delegate your compliance actions. Within the framework of its outsourced services, CyberSecura issues expert recommendations, but the client always remains free to make the decisions he wishes.

The two main components of this service

A compliance component, with the writing of all the compliance documentation, the processes for exercising IT rights and freedoms, the texts of information for the persons concerned, and the mandatory contractual texts in the context of subcontracting.

A support component, with full availability to answer questions from company employees, answer questions from customers/prospects, ensure an adequate response to requests to exercise Data Protection Rights, answer questions about the feasibility of actions by the organisation, etc.

Support is a priority, and documentation is a gradual process.

This service allows you to benefit from a badge designed to highlight your commitments. These badges have a communication objective and you can use them freely on all the media that you consider relevant!

Macaroons also available in English

Copyright © CyberSecura 2024 - All rights reserved

DRAFTING THE COMPLIANCE DOCUMENTATION

Towards a governance of GDPR regulatory compliance

Regulatory compliance with the GDPR requires the implementation and development of specific documentation. This documentation includes elements aimed at informing your customers, partners and prospects of the personal data processing carried out by your organisation. But it is also essential in the event of an inspection by the CNIL and in order to demonstrate your pro-activity and your efforts to comply with the regulations.

Within the framework of an outsourced DPO service, our experts draft for you

Privacy Policy

to inform Internet users of the data processing carried out on your website.

Contractual clauses for subcontractors and employees

to contract the regulatory obligations of your partners and subcontractors.

Letter of commitment to compliance

to your clients, prospects or any other partner who requests it.

Mandatory information

in your emailings, but also on the contact forms on your website.

Register of requests to exercise data protection rights

in order to record all requests for the exercise of Data Protection Rights.

Register of data processing operations

to list all data processing carried out by your organisation.

Data Protection Impact Assessment (PIA)

to build compliant, ethical and privacy-friendly data processing.

Etc.

Make the most of your commitments

Macaroons also available in English

Copyright © CyberSecura 2024 - All rights reserved

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, FRANCE

+33 (0)6 21 54 42 37

www.cybersecura.com

contact@cybersecura.com

Copyright © CyberSecura 2024 - All rights reserved