Punto della situazione

Domande orientative per la propria organizzazione

# Da compilare da parte della divisione IT/OT interna:

|  |  |
| --- | --- |
| Nome del fornitore: |  |
| Prestazione del fornitore: |  |
| Interlocutore all’interno della propria organizzazione: |  |
| Contatto: |  |
| Questionario n.: |  |

# Prestazioni del fornitore

| 1.1 | Le prestazioni del fornitore o del partner sono importanti per i nostri processi aziendali? | Sì  No  Non lo so |
| --- | --- | --- |
|  | Descrivere le prestazioni. |  |

# Prodotti IT/OT del fornitore

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.1 | Il fornitore ci fornisce prodotti IT od OT che operano nei nostri ambienti (critici)? | | Sì ☐  No ☐  Non lo so☐ | |
|  | | Descrivere i prodotti IT/OT. |  |

# Accesso dei fornitori ai sistemi interni

| 3.1 | Il fornitore ha accesso a sistemi (critici) da noi operati? | Sì ☐  No ☐  Non lo so☐ |
| --- | --- | --- |
|  | Se la risposta è affermativa, specificare il tipo di dati memorizzati in questi sistemi. |  |
|  | Dati interni alla nostra organizzazione | Sì ☐  No ☐  Non lo so☐ |
|  | Dati aziendali interni, compresi i dati dei clienti e dei partner della nostra organizzazione. | Sì ☐  No ☐  Non lo so☐ |
|  | Dati sui collaboratori della nostra organizzazione | Sì ☐  No ☐  Non lo so☐ |
|  | Dati personali di clienti/partner della nostra organizzazione | Sì ☐  No ☐  Non lo so☐ |
|  | Dati di identificazione dei collaboratori (password) della nostra organizzazione | Sì ☐  No ☐  Non lo so☐ |
|  | Altro. |  |
| 3.2 | Se applicabile nella propria organizzazione: Il fornitore ha effettuato controlli personali sui collaboratori che hanno accesso ai sistemi informatici gestiti all’interno delle reti IT della nostra organizzazione o ai sistemi informatici che elaborano i dati della nostra organizzazione prima di concedere l’accesso a tali sistemi informatici? | Sì ☐  No ☐  Non lo so☐ |
|  | Se la risposta è negativa, si prega di adeguare di conseguenza la componente contrattuale «Attribuzione dei diritti». |  |

# Sistemi gestiti dal fornitore

| 4.1 | Il fornitore gestisce per conto nostro i sistemi di cui necessitiamo per i processi aziendali critici? Si tratta, ad esempio, di applicazioni basate su SaaS per il reclutamento, payroll o i sistemi di collaborazione. | | Sì ☐  No ☐  Non lo so☐ |
| --- | --- | --- | --- |
| 4.2 | | Quali dati vengono raccolti o salvati in questo contesto? |  |
|  | | Dati personali (cognome, nome, data di nascita, luogo di nascita, numero AVS, numero di passaporto o di carta d’identità, indirizzo, numero di telefono, indirizzo e-mail, indirizzi IP di ubicazioni, ecc.) | Sì ☐  No ☐  Non lo so☐ |
|  | | [[1]](#footnote-1)Dati personali degni di particolare protezione (informazioni sulla salute, sulla religione, sulle opinioni politiche e ideologiche, sull’orientamento sessuale e sulla privacy, dati biometrici e genetici, casellario giudiziario, ecc., ai sensi della vigente legge federale sulla protezione dei dati) | Sì ☐  No ☐  Non lo so☐ |
|  | | Dati della carta di credito | Sì ☐  No ☐  Non lo so☐ |
|  | | Dati di connessione (indirizzo IP, geolocalizzazione, dati di posizione GPS, altri dati di telemetria, ecc.) | Sì ☐  No ☐  Non lo so☐ |

# Ciberattacco al fornitore

Queste domande sono pertinenti se le prestazioni del fornitore sono rilevanti per il processo aziendale o se vengono trattati i dati dell’organizzazione.

| 5.1 | La nostra organizzazione garantisce di essere in grado di evitare una perdita di dati in caso di un grave ciberattacco al fornitore? | Sì ☐  No ☐  Non lo so☐ |
| --- | --- | --- |
|  | In caso di risposta negativa, descrivere le misure previste (ad es. isolamento / monitoraggio degli accessi / MFA). |  |

|  |  |  |
| --- | --- | --- |
| 5.2 | Siamo in grado di continuare a gestire i nostri processi aziendali se il fornitore non è disponibile (per un periodo prolungato)? | Sì ☐  No ☐  Non lo so☐ |
|  | In caso di risposta negativa, descrivere le misure previste (ad esempio, come affrontare un’interruzione di corrente / piano di emergenza / backup offline): |  |
| 5.3 | Siamo in grado di continuare a offrire i nostri processi aziendali se il fornitore non è disponibile (per un periodo prolungato)? | Sì ☐  No ☐  Non lo so☐ |
|  | Se la risposta è negativa, descrivere le misure previste (ad esempio, come affrontare un’interruzione di corrente / piano di emergenza): |  |

1. L’espressione «Dati degni di particolare protezione» comprende tutti i dati che, se pubblicati, potrebbero comportare un rischio elevato per le persone fisiche interessate. [↑](#footnote-ref-1)