REGIONE DEL VENETO

AZIENDA ZERO

Misure di Sicurezza

Misure di Sicurezza atte alla finalizzazione della nomina privacy

#	MISURE DI SICUREZZA
1	L'Organizzazione adotta un Sistema di gestione della Privacy, definisce e assegna ruoli e responsabilità delle figure coinvolte, adotta procedure e policies formalizzate e aggiornate in materia di protezione dei dati personali e di sicurezza delle informazioni.
2	L'Organizzazione, coerentemente con il Sistema di gestione della Privacy adottato, adotta gli strumenti e i presidi previsti dalla normativa, tra cui, qualora ne ricorrano i presupposti, il Registro dei trattamenti.
3	A livello organizzativo, sono individuate le aree responsabili della gestione degli aspetti relativi alla privacy (es. uffici / strutture preposte, personale dedicato, ecc.) e, nel caso in cui ricorrano i requisiti previsti dalla legge, è stato individuato e nominato un DPO/RPD in conformità con quanto previsto dal GDPR.
4	Agli autorizzati al trattamento sono impartite istruzioni scritte che definiscano le modalità di gestione dei dati personali oggetto di trattamento.
5	Sono previste e attuate attività di formazione sui temi di sicurezza e privacy nei confronti degli autorizzati al trattamento.
6	Le attività di trattamento svolte dai Responsabili del trattamento sono disciplinate da appositi accordi scritti, e sono definite apposite attività di monitoraggio / riesame dei Responsabili esterni.
7	L'Organizzazione, ove opportuno, definisce e adotta informative adeguate e conformi a quanto previsto dalla normativa vigente (es. espresse in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro).
8	I sistemi sono configurati in modo tale che, per impostazione predefinita, siano visibili e accessibili da parte degli incaricati al trattamento solo i dati personali necessari per ogni specifica finalità del trattamento (c.d. principio di "privacy by default").

9	La società ha definito una procedura per la valutazione degli impatti privacy delle attività/progetti svolti, incluse le attività di sviluppo/change (c.d. principio di "privacy by design").
10	Sono individuati, designati e gestiti i soggetti che operano in qualità di Amministratori di Sistema in conformità con quanto previsto dal provvedimento del 27/11/2008 del Garante Privacy. Inoltre, è predisposto e aggiornato periodicamente un elenco degli stessi con le relative responsabilità e i compiti assegnati.
11	Gli access log degli Amministratori di Sistema sono gestiti in conformità con quanto previsto dal provvedimento del 27/11/2008 dell'Autorità Garante sugli Amministratori di Sistema.
12	I sistemi IT utilizzati dall'Organizzazione sono catalogati sulla base delle informazioni contenute negli stessi (classificazione dei dati) .
13	Alla fine del loro ciclo di vita, gli asset IT utilizzati per l'elaborazione dei dati sono dismessi in modo sicuro (sovrascrittura/cancellazione logica, etc.).
14	Le attività di backup svolte dall'Organizzazione sono effettuate con frequenza predeterminata e adeguata a garantire la disponibilità dei dati in conformità al livello di criticità degli stessi.
15	L'Organizzazione ha definito un piano di Disaster Recovery e un processo di Business Continuity, e questi sono periodicamente aggiornati.
16	È definito e documentato un processo di gestione delle utenze (es. creazione utenza, profilazione, variazione di mansione, dismissione utenza) che identifichi anche i relativi ruoli e responsabilità.
17	L'Organizzazione assicura che le utenze dei dipendenti che lasciano la società siano disattivate in modo permanente.
18	L'Organizzazione ha definito un processo per cui gli accessi agli applicativi (logon / logoff) sono tracciati e adeguatamente protetti da azioni/modifiche indesiderate.
19	Il controllo accessi è basato su una politica che correla l'accesso alle informazioni alle effettive esigenze lavorative (principio need to know).
20	L'Organizzazione fornisce ad ogni utente un'utenza individuale, univoca e non riassegnabile ad altre persone.
21	L'Organizzazione adotta adeguati presidi per la gestione degli accessi ai sistemi IT, tra cui la limitazione al numero di tentativi di accesso non andati a buon fine, valutazione sull'utilizzo di tecniche di autenticazione multifattore, etc. .
22	Le credenziali per l'accesso al sistema sono archiviate in maniera adeguatamente protetta (es. cifratura delle password di dominio).

23	Le password utilizzate devono rispettare un livello di complessità conforme ai più recenti standard di sicurezza ed essere soggette ad una scadenza periodica non superiore ai 90 giorni.
24	Esiste una procedura per la distribuzione sicura agli utenti delle password di accesso (es. invio delle password all'interno di buste sigillate, comunicazione delle stesse tramite un canale diverso da quello utilizzato per la comunicazione dell'utenza (email personale), ecc.).
25	L'Organizzazione effettua attività di revisione periodica dei diritti di accesso ai dati affinché l'assegnazione dei profili sia coerente con le mansioni attribuite.
26	L'Organizzazione utilizza ambienti di sviluppo e test separati dall'ambiente di produzione ed evita l'utilizzo di dati reali al di fuori dell'ambiente di produzione.
27	Sono adottate le politiche previste per lo sviluppo sicuro del software (es. secure coding guidelines, politiche e procedure, ecc.), in coerenza con best practice e standard di settore internazionali.
28	L'Organizzazione svolge con cadenza periodica attività di vulnerability assessment e/o penetration test.
29	L'Organizzazione adotta misure di sicurezza fisica per l'accesso, il monitoraggio e il mantenimento in sicurezza di edifici e sala server (es. accesso con chiavi, badge, tornelli, telecamere, sistema di allarmistica antintrusione e antincendio, ecc.).
30	L'Organizzazione ha definito una procedura per la gestione e archiviazione della documentazione cartacea.
31	Le informazioni e i dati trattati, anche cartacei, vengono protetti con adeguate misure di sicurezza, come la chiusura a chiave degli armadi, l'uso di armadi ignifughi e sistemi di rilevazione del fumo. Il personale autorizzato all'accesso deve prestare attenzione e cura nel mantenere queste misure di sicurezza.
32	Sono adottati processi per l'identificazione, valutazione e gestione delle vulnerabilità delle risorse (es. sistemi, locali, dispositivi).
33	L'Organizzazione ha definito un processo di gestione degli incidenti che consenta di rilevare, registrare, gestire e chiudere eventuali incidenti di sicurezza informatica.
34	L'Organizzazione ha definito un processo di gestione degli incidenti di sicurezza che impattano sui dati personali (data breach), nel rispetto della normativa vigente e che preveda una comunicazione tempestiva degli incidenti ad organizzazioni terze nel caso in cui vengano svolte attività di trattamento di dati personali per loro conto.
35	L'accesso wireless al sistema IT è consentito solo a utenti autorizzati dall'Organizzazione, utilizzando canali sicuri ed adeguatamente protetti (es. meccanismi di crittografia sicuri). Il

	traffico di rete è comunque monitorato e controllato attraverso Firewall e Intrusion Detection Systems.
36	L'Organizzazione adotta procedure di gestione dei dispositivi mobili e portatili stabilendo regole chiare per il loro corretto utilizzo e individuando ruoli e responsabilità specifici relativi alla loro gestione.
37	L'Organizzazione adotta e mantiene aggiornate soluzioni tecnologiche di protezione dalle minacce esterne (es. antivirus, antispam, content filtering, ecc.) sulle postazioni di lavoro e sulla rete dati.
38	Sono garantite comunicazioni sicure secondo le best practices attuali (ad es. adozione di HTTPS, SSL e certificati EV (Extended Validation Certificate).
39	L'Organizzazione considera la cifratura dei dati *at rest* (es. a livello di disco o di database) sulla base di una valutazione della criticità dei dati salvati.
40	L'Organizzazione definisce e attua un processo di monitoraggio periodico per identificare e installare tempestivamente le patch (anche provenienti da fornitori).