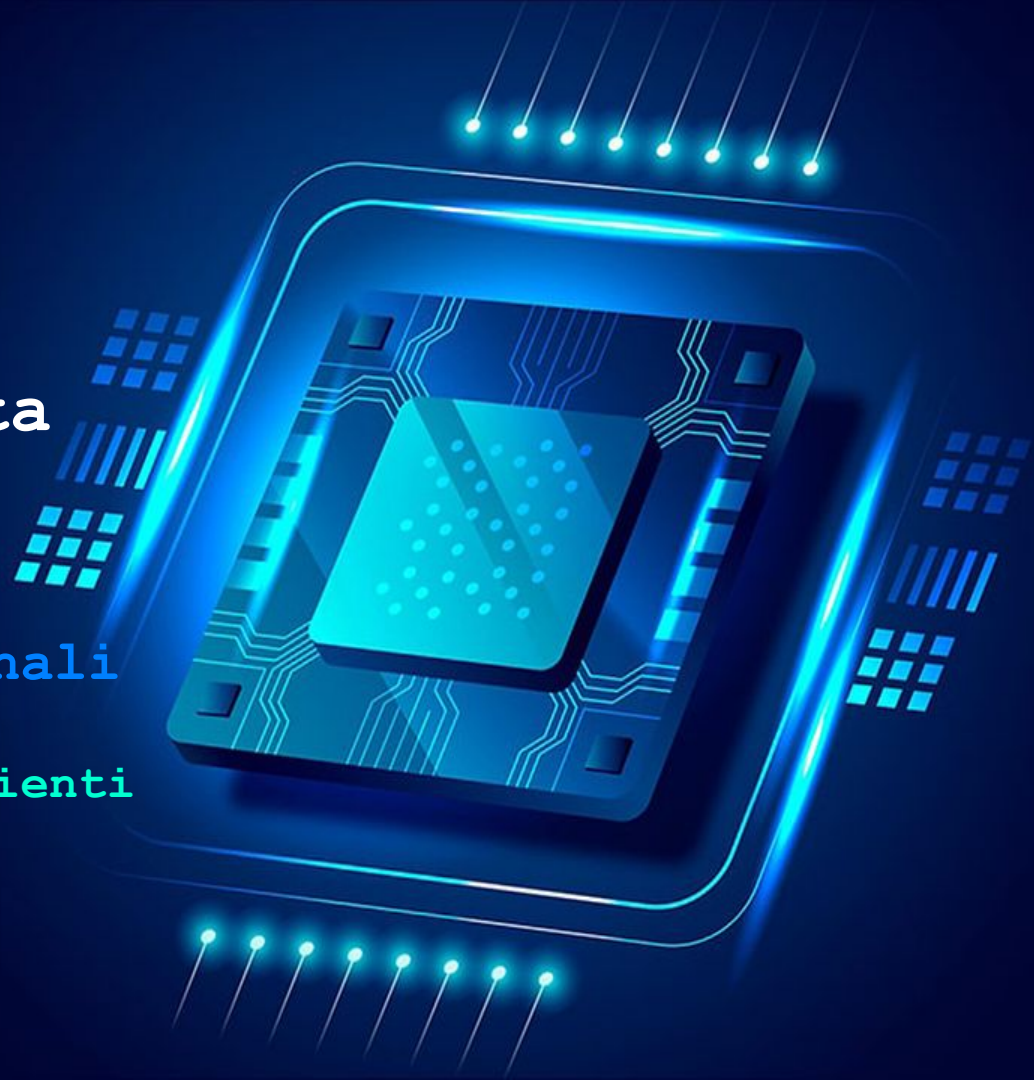


// codice di condotta

Software House e gestionali
Scrivere codice conforme
Gestire i rapporti con i clienti



Agenda

Introduzione
Chi, cosa, dove
Progettazione
Sviluppo
Installazione, manutenzione, assistenza
Cosa non riguarda
I ruoli della software house

Progettazione e sviluppo
Ruolo della SwH
Come progettare e sviluppare
Le misure dell'Allegato A
Installazione, manutenzione, assistenza
Il Ruolo in cloud e on premise
Amministratore di Sistema
Il DPA
I sub Responsabili
Le misure dell'Allegato B

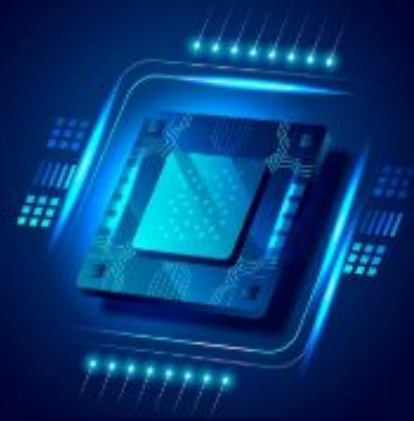
Altri obblighi della SwH
Analisi rischi
Misure di sicurezza
Incidenti
Personale
Riscontro diritti
Trasferimenti
Data retention
Informazioni e verifiche del cliente

E' stato pubblicato, sulla [Gazzetta Ufficiale](#), il **Codice di Condotta** destinato ai **produttori di software gestionali** (Sw House) che ha lo scopo di garantire che l'intero ciclo di vita del software sia rispettoso delle regole sulla protezione dei dati personali.

L'obiettivo è quello di **favorire la compliance data protection** e di **aumentare la fiducia degli utilizzatori**.

Il Codice è stato elaborato da Assosoftware in collaborazione con il Garante della Privacy.

// Regole uniformi



Misure tecniche e organizzative

Conformità data protection

Chi

Software House

Produttori di sw gestionali

Cosa

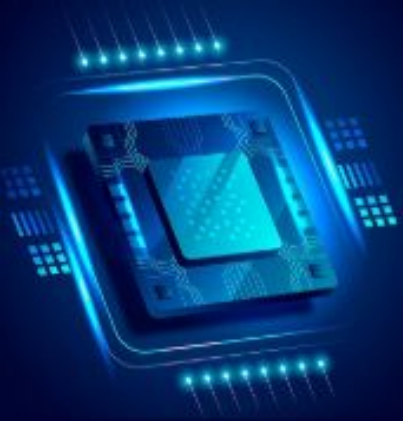
Sviluppo di gestionali

Installazione, assistenza, manutenzione

Dove

On premise, in cloud, anche da remoto





Allegato C - DPA

Allegato B

Amministratore di Sistema

On premise - In cloud

SWHouse è Responsabile (o Sub)

Progettazione

Produzione

Sviluppo

Installazione

Messa in
esercizio

SW House, Produttore, è Titolare del trattamento

Deve sviluppare secondo Privacy by Design e by
Default

Allegato A

// Progettazione



Analisi requisiti

Progettazione architettura

Progettazione interfaccia

// Sviluppo

Codifica

Testing

Integrazione

Deployment



// Installazione, manutenzione assistenza



Installazione e configurazione

Test e collaudo

Assistenza e correzione

Aggiornamenti, patch, manutenzione



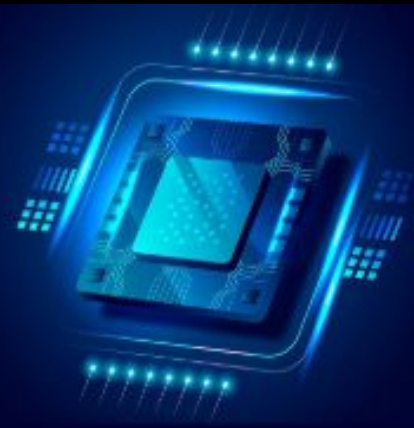
NON riguarda

Elaborazione dati per conto del cliente

Es.: gestione contabilità, gestione rapporti previdenziali, ecc.



Software House/1



Titolare

Produce, progetta, sviluppa, vende

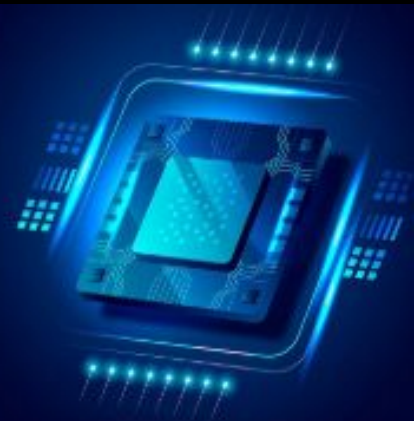


Il Cliente





Software House/2

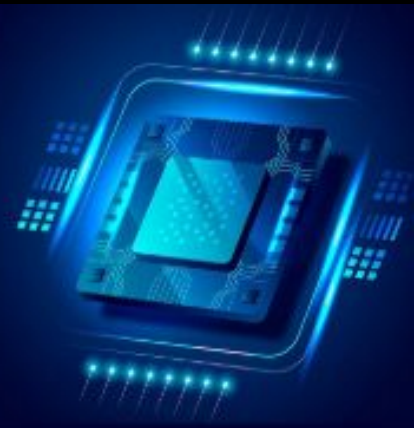


Responsabile Installa, mantiene, fa assistenza

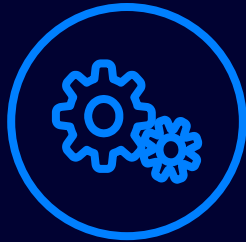


Si avvale di fornitori: Sub Responsabili

Software House/3



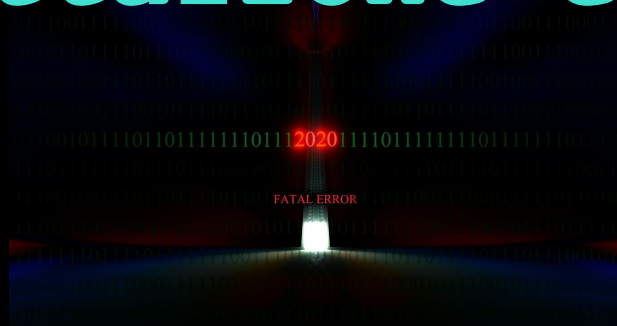
Il Cliente è un
Responsabile



Sub Responsabile

Installa, mantiene,
fa assistenza

// Progettazione e sviluppo



La Sw House è titolare del trattamento

Tratta i dati del cliente per la gestione contrattuale.

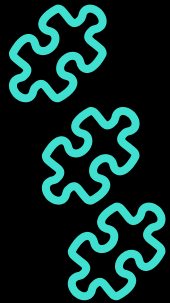
Può effettuare analisi dei dati dei clienti e dei relativi utenti (uso del sw e relative funzionalità) in forma aggregata sulla base del legittimo interesse.

Le finalità sono di miglioramento prestazioni e sicurezza.

Adotta, però, tecniche di pseudonimizzazione.



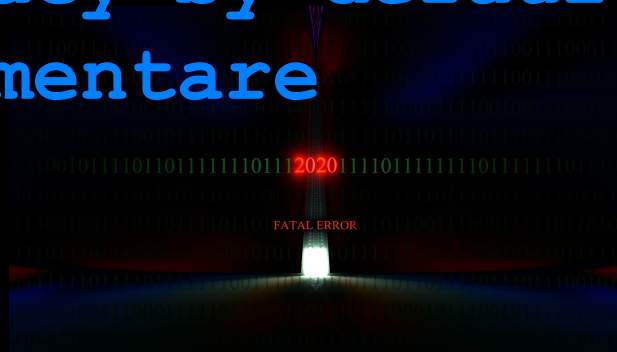
Come progettare e sviluppare



Privacy by design

Privacy by default

Documentare





Valutazione dei rischi dei trattamenti del gestionale



Funzionalità, misure tecniche e organizzative per consentire al cliente di garantire la protezione dei dati



Comunicazione trasparente al cliente delle funzionalità





Adottare le misure di cui
all'Allegato A



Allegato A

Definisce **i principi fondamentali** per lo sviluppo di software gestionale secondo i criteri di **privacy by design e by default**.

Si articola in otto macro-aree che coprono l'intero ciclo di vita del software:

- 1) analisi delle funzionalità,
- 2) protezione accesso ai dati,
- 3) gestione degli accessi,
- 4) autenticazione,
- 5) protezione degli archivi del cliente,
- 6) sicurezza del codice,
- 7) requisiti sistemistici,
- 8) ambienti di test.

Ogni area prevede **controlli specifici**.

Privacy by Design



Linee guida di riferimento

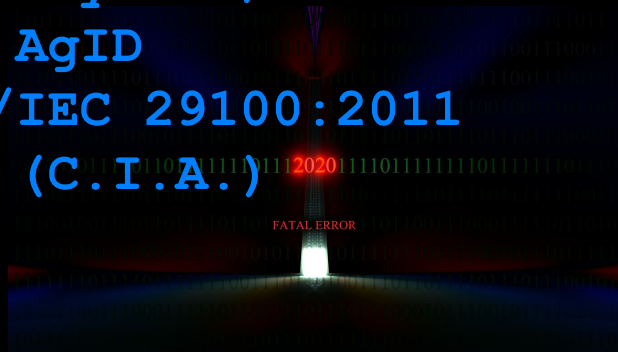
Controlli UNI CEI ISO/IEC 27002:2022

Controlli privacy ISO/IEC 27701:2019

Misure Minime AgID

Misure da ISO/IEC 29100:2011

Triade R.I.D. (C.I.A.)





Ambito	Catalogazione	Requisito di dettaglio
Principi di sviluppo del SW Gestionale	Analisi di nuove funzioni	Valutazione e documentazione nelle analisi delle funzioni applicative del rispetto dei principi di minimizzazione: - nel dato: ogni dato personale raccolto dal SW deve essere necessario rispetto alla finalità della raccolta - nell'uso: ogni dato personale deve essere trattato solo da coloro che ne abbiano un'effettiva necessità - nel tempo: il dato personale deve essere trattato per il tempo strettamente necessario per il perseguimento della finalità. In particolare, già in fase di analisi devono essere identificati i dati personali trattati, la durata prevista dal trattamento, l'indicazione dei ruoli che vi potranno accedere, l'indicazione dei processi che vi potranno accedere, l'indicazione degli output.



Definizione della protezione dell'accesso ai dati	Documentazione degli strumenti e dei requisiti per l'utilizzo del SW	Documentazione degli strumenti utilizzati per trattare i dati (indicazione del DB utilizzato, strumento di scrittura del codice, sistema di conservazione dei documenti prodotti), definendo le misure di sicurezza poste a tutela dei dati (profili di accesso al DB, crittografia del DB, dialogo tra applicazione e DB e protezione delle password, ecc.). Documentazione dei sistemi operativi e dei requisiti per l'utilizzo del SW.
Autenticazione	Modalità e regole di autenticazione	Utilizzo di utenze nominative individuali al fine di garantire la tracciabilità delle operazioni eseguite. Conformità della password policy alle best-practice europee e internazionali di riferimento che ne garantiscano sicurezza adeguata, sia in termini di complessità (es. minimo 8 caratteri presenza di caratteri speciali, maiuscole, etc.), scadenza (durata fissa o modulabile dal cliente/titolare del trattamento), ciclicità della password (es. non consentire il riuso di password precedenti), gestione reset delle password con sistemi che garantiscano l'identificazione del richiedente e simili. Adozione di misure per prevenire e contrastare attacchi informatici di tipo credential stuffing (testing username/password pairs obtained from



		the breach of another site), brute force (testing multiple passwords from dictionary or other source against a single account) e password spraying (testing a single weak password against a large number of different accounts).
	MF Authentication	MFA (quali ad es. OTP, smartcard ecc.) implementabili in base al livello di rischio dei trattamenti di dati personali e alle prescrizioni delle norme di riferimento. Tra i fattori di autenticazione prevedere anche la possibilità di autenticare anche il singolo device che si collega in relazione alla rischio del trattamento.
	Gestione accessi	Adozione di misure che consentono di monitorare e gestire i rischi inerenti agli accessi ai sistemi applicativi, tra cui, a titolo esemplificativo: - disattivazione delle credenziali in caso di inutilizzo per tempi prolungati (es.: sei mesi); - disattivazione temporanea o definitiva in caso di superamento di un numero impostato di tentativi di accesso falliti reiterati;



		- impostazione di time out della sessione attiva; - visualizzazione data e ora ultimi accessi; - salvataggio dei log di accesso al sistema in modo che i clienti possano esportarli a sistemi terzi di conservazione che ne garantiscano l'integrità e la conservazione per i tempi definiti dai clienti stessi.
	API	Adozione di misure di autenticazione per le API (es.: certificato digitale; token, ecc.).
Profili di accesso	Profili di accesso	Gestione delle utenze, sia utilizzate dal cliente per effettuare attività di amministratori del sistema (ad esempio per essere autonomi nella generazione delle utenze o nell'impostare parametri di utilizzo), sia per l'utilizzo del sistema stesso, in conformità a procedure volte a garantire il rispetto del principio di minimo privilegio e un'adeguata segregazione dei compiti gli utenti devono accedere solo a funzioni, file di dati, URL, controller, servizi e altre risorse, per le quali possiedono un'autorizzazione specifica. Le eventuali utenze generate per far accedere gli incaricati del trattamento del fornitore al fine di prestare assistenza sul prodotto utilizzato saranno identificate nominalmente e avranno profilo di accesso amministrativo e saranno gestite dal cliente con relativa attivazione



		e disattivazione in caso di necessità di utilizzo.
Autenticazione	Gestione delle autorizzazioni	Inventario delle utenze presenti nel sistema con i relativi profili di autorizzazione assegnati, disponibile al cliente per sua rendicontazione e analisi degli accessi.
Protezione archivi dati Cliente	Protezione dati Cliente	Adozione di tecniche di pseudonimizzazione o cifratura dei dati (tokenizzazione, etc.) adottabili dal Cliente ove appropriate allo scopo di garantire un adeguato livello di protezione in relazione alle tipologie di dati personali trattati (es.: categorie particolari ex art. 9 del GDPR e dati penali ex art. 10).



Protezione archivi	Protezione archivi contenenti le password	Adozione, per la conservazione delle password degli utenti, di adeguate tecniche crittografiche quali le funzioni di derivazione di chiavi crittografiche (Key Derivation Function) che offrono garanzie in caso di loro esfiltrazione dai sistemi informatici del Produttore (cfr. OWASP Password Storage Cheat Sheet, NIST 800-63B Digital Identity Guidelines).
Sicurezza SW	Secure coding	Adozione di policy e procedure finalizzate a garantire che lo sviluppo degli applicativi avvenga nel rispetto di linee guida di secure coding conformi alle best practices (quali, ad es., OWASP, controllo delle librerie di terze parti costante e identificazione di eventuali criticità con segnalazione ai clienti e sostituzione immediata delle librerie che comportano criticità nel trattamento dei dati, etc.).
	Minacce e Vulnerabilità	Test di penetrazione con cadenza periodica (quantomeno al rilascio di ogni major release), se il SW è destinato ad essere esposto su reti pubbliche Adozione di un piano di miglioramento che analizzi le vulnerabilità emerse dai VA e PT e dai bollettini di sicurezza pubblici e di fornitori terzi e ne preveda una adeguata gestione/risoluzione.



		Svolgimento periodico di analisi di vulnerabilità.
Requisiti sistemistici e di gestione	Log applicativi di attività utente	Funzionalità per il tracciamento del log degli accessi e delle attività svolte in relazione alle diverse tipologie di utenza (amministratore, super utente, utente, etc.) allo scopo di consentire al titolare o al responsabile del trattamento un'adeguata attività di monitoraggio. I log riguardanti le attività svolte devono essere opportunamente protetti a garanzia della loro integrità e riservatezza. Tali funzionalità devono essere attivabili da parte dell'amministratore del sistema del Cliente.



Ambienti di test	Misure per ambienti di test	
		Separazione degli ambienti di test e sviluppo rispetto ad ambienti di produzione e previsione di misure di accesso mediante credenziali e privilegi diversi in modo di ridurre al minimo i rischi.



Funzioni specifiche	Data retention	
		Previsione di funzioni del SW che consentano ai clienti di impostare la cancellazione dei dati personali trascorso il periodo necessario di loro conservazione. Il SW deve prevedere estrazioni di dati che consentano ai clienti di essere consapevoli sui periodi di conservazione dei dati al fine di trattare i dati secondo il principio di minimizzazione.



Funzioni specifiche	Portabilità	Funzionalità idonee a consentire al Cliente l'estrazione dei dati personali in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo in caso di esercizio del diritto alla portabilità da parte dell'interessato, ove ne ricorrano i presupposti.
Misure organizzative	Formazione	Erogazione periodica alle persone autorizzate al trattamento di corsi di formazione sulla sicurezza e protezione dei dati personali. Per gli sviluppatori sono previsti anche corsi di sviluppo sicuro.
Misure di sicurezza	Backup	Funzionalità al fine di permettere al Cliente di effettuare, anche tramite processi esterni, il salvataggio o backup dei dati trattati dall'applicativo.



Misure di sicurezza	Esattezza e accuratezza dei dati	Adozione di misure per assicurare al Cliente una verifica dell'esattezza e dell'accuratezza dei dati (ad es. controlli di correttezza formale della PIVA o CF).
---------------------	----------------------------------	---



Misure di sicurezza	Riservatezza dei dati	Adozione di misure per agevolare il Cliente nel rispetto del requisito della riservatezza in caso di utilizzo di funzioni di condivisione dei dati (tramite ad es. l'invio di avvisi o notifiche).
Misure organizzative	Inventory Librerie	Conservazione dell'inventario delle componenti software in uso comprensive delle librerie di terzi e/o open source in modo da poter rispondere più tempestivamente in caso di segnalazioni di vulnerabilità (SBOM SW bill of materials).



Misure organizzative	Change management	Regolamentazione del processo di gestione delle modifiche applicative ed infrastrutturali, al fine di garantire un miglior presidio di ogni fase del ciclo di vita del SW e di tracciarne l'evoluzione, con monitoraggio dei livelli di accesso alle informazioni critiche e adeguata formazione/sensibilizzazione delle persone coinvolte nel processo di Change Management (al rispetto dei principi di <i>Segregation of Duties</i>).
Misure organizzative	Configuration management	Regolamentazione del processo di Configuration management al fine di garantire la corretta gestione delle versioni dei rilasci dei moduli SW.
Misure di sicurezza	Trasmissione dati personali	Utilizzo di protocolli sicuri e adeguati allo sviluppo tecnologico per proteggere i dati durante la loro trasmissione.



Misure di sicurezza	File temporanei	Funzionalità per permettere l'eliminazione dei file temporanei contenenti dati personali e creati durante i trattamenti e cancellazione sicura dei dati sugli strumenti dismessi (<i>Secure disposal</i>).
---------------------	-----------------	--



// Installazione,
manutenzione, assistenza

In cloud



Sw House Responsabile del trattamento

Se il cliente è un responsabile, diviene
sub-responsabile

On premise



Responsabile del trattamento

O sub Responsabile **solo se** effettua **attività tecniche** (install. gest. assist.) che comportino il **trattamento** di dati personali.

Esempi:

- migrazione dati
- assistenza e aggiornamento con accesso a dati
- acquisizione, estrazione, copia di basi dati

```
..
0. Sep 15:53 bin -> usr/bin
19. Sep 09:31 boot
19. Sep 15:50 dev
21. Sep 09:32 etc
7 30. Sep 2015 home
7 30. Sep 2015 lib -> usr/lib
34 23. Jul 10:01 lib64 -> usr/lib
96 1. Aug 22:45 lost+found
96 30. Sep 2015 mnt
16 21. Sep 2015 opt
0 21. Sep 15:52 private -> /home/encrypted
4096 12. Aug 15:37 proc
560 21. Sep 15:50 root
7 30. Sep 2015 run
4096 30. Sep 2015/sbin -> usr/bin
t 0 21. Sep 2015 srv
rt 300 21. Sep 15:51 sys
4096 12. Aug 15:45
4096 23. Jul 10:25 usr
16 4096 21. Sep 15:52 var
```

Amministratori di Sistema

In caso di assistenza e manutenzione continuative.



Gestione e manutenzione
infrastruttura, sicurezza fisica e
logica, backup e ripristino, non
competono alla Swh



Non determina i presupposti di liceità dei trattamenti effettuati con il gestionale.



Può rifiutarsi di effettuare operazioni palesemente illegittime.





Stipulare un **DPA**, un accordo per
il trattamento in qualità di
Responsabile come da **Allegato C**

Il DPA (estratto)

SCHEMA DI ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679 - REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI¹

TRA
 _____ (indicare Cliente) con sede legale in
 _____ (di seguito anche il "Cliente"),
 da una parte,

E
 _____ (indicare SWH) con sede legale in
 _____ (in seguito anche la "Software House" o "SWH"),
 dall'altra parte,

(il Cliente e la SWH, indicati di seguito, singolarmente, come la "Parte" e, collettivamente, come le "Parti").

Premesso che:

- le Parti hanno sottoscritto un contratto (di seguito "Contratto") di concessione della licenza d'uso del Software gestionale sviluppato e prodotto dalla SWH e di svolgimento dei Servizi di cui all'art. 2, comma 1, lett. c) del Codice di condotta, come specificati nel Contratto che possono comportare operazioni di trattamento di dati personali eseguite dalla medesima SWH per conto del Cliente;
- in relazione alle suddette operazioni di trattamento di dati personali, il Cliente riveste dunque il ruolo di Titolare del trattamento [o di "Responsabile del trattamento"]², mentre la SWH opera in qualità di Responsabile del medesimo trattamento [o di "Sub-responsabile del trattamento"] ai sensi dell'art. 28 del Regolamento (UE) 2016/679 - Regolamento Generale sulla Protezione dei Dati (di seguito il "Regolamento" o "GDPR")³;
- in particolare, la SWH dichiara, ai sensi dell'art. 28, comma 5, del GDPR, di aderire al "Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale" (di seguito il "Codice di condotta") e pertanto dichiara di mettere in atto misure tecniche ed organizzative adeguate al fine di garantire che il suddetto

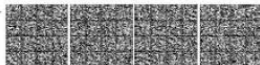
¹ Si riporta qui di seguito il testo esemplificativo di articolo da inserire nel Contratto con il Cliente, contenente il rinvio allo schema di Accordo sul trattamento dei dati personali da allegare al medesimo Contratto.

*Art. ... - Trattamento dei dati personali

In relazione al trattamento dei dati personali connesso allo svolgimento dei Servizi, il Fornitore conferma di svolgere tale trattamento in qualità di Responsabile/Sub-responsabile per conto del Cliente, quale Titolare/Responsabile del medesimo trattamento, e, ai sensi dell'articolo 28 del Regolamento, si impegna a garantire il rispetto degli obblighi previsti nell'Accordo sul trattamento dei dati personali di cui all'Allegato ..., contenente anche la descrizione del suddetto trattamento dei dati personali. (...)

² Sostituito con "Responsabile del trattamento", ove il Cliente agisca invece in tale qualità per conto di un soggetto terzo quale Titolare, adeguando anche le successive parti in cui si indica il Cliente quale Titolare del trattamento (da sostituire, in tal caso, con "Responsabile del trattamento").

³ Inserire l'ulteriore Responsabile del trattamento (di seguito "Sub-Responsabile")³, ove, come indicato al precedente commento, il Cliente agisca già quale Responsabile del trattamento e uniformare anche tutte le successive parti (sostituendo il termine di "Responsabile" riferito alla SWH con "Sub-Responsabile").



Allegato A

Descrizione delle attività di trattamento di dati personali connesse allo svolgimento delle Attività oggetto del Contratto

Attività svolte	Finalità del trattamento	Natura del trattamento	Durata del trattamento	Categorie di interessati	Categorie di dati personali
Es.: installazione, test, collaudo, messa in esercizio, assistenza, manutenzione, aggiornamento del SW Gestionale ...	---	Interamente/parzialmente automatizzata	Es.: Durata del Contratto	Es.: clienti, utenti, dipendenti, ecc.	Es.: dati personali comuni, dati particolari, dati penali (specificare sotto categorie) ...

L'Allegato



Accordo uniforme per pluralità di clienti

E' possibile proporre uno schema generale destinato a regolare rapporti uniformi con una pluralità di clienti.



I Sub Responsabili della SW House



Cliente



SoftwareHouse



SubFornitore

Affida alla
software house
attività,
prestazioni e
servizi

Esegue attività
di installazione,
manutenzione,
assistenza e **si**
avvale di
ulteriori
fornitori

Attività e
servizi (con
trattamento di
dati) **dipendenti**
dal rapporto tra
SwH e Cliente

Ci vuole autorizzazione del cliente

Nel DPA

Riferita a categorie e tipologie di servizi

Elenco nominativo da fornire su richieste del cliente

Elenco modificabile con congruo preavviso al cliente

Il cliente può opporsi alla modifica entro 30 gg.

Elenco dei Sub Fornitori



Nominativo
Denominazione
legale



Sintetica
descrizione del
trattamento



Luogo del
trattamento



Disponibile per
il cliente



Accordi di riservatezza
Richiedibili al Cliente



Impegni e facoltà della SwH



Trasferire i
medesimi obblighi
in tema di misure
tecniche e
organizzative



Il Cliente può
opporsi



Utilizzare
provider con
accordi non
negoziabili



Comunicandolo al
cliente.

Facendo ogni
sforzo per la
verifica delle
Condizioni.





Adottare le misure di cui
all'**Allegato B**

Allegato B

Le misure delineano i **requisiti di sicurezza** che il produttore deve implementare nell'erogazione dei servizi di assistenza, sia in ambiente on premise che cloud.

Per le installazioni **on premise**, i controlli si concentrano sulla gestione degli accessi, sicurezza logica, monitoraggio, supporto remoto e governance degli archivi.

Nel contesto **cloud**, l'attenzione si sposta sulla sicurezza dell'infrastruttura del data center, connettività, protezione della rete e requisiti sistemistici. In entrambi gli scenari, la governance assume un ruolo centrale per garantire la corretta applicazione delle misure di sicurezza.



On premise



Ambito	Catalogazione	Requisito di dettaglio
Gestione Account	Autorizzazione autenticazione	Tutti gli operatori della SWH devono accedere alle piattaforme utilizzate per l'assistenza previa autenticazione con le credenziali nominative individuali. Nel caso di un tentativo d'accesso alla piattaforma di supporto con un account diverso da quello autorizzato, il sistema deve negare l'accesso. Le utenze degli operatori incaricati dell'assistenza sono periodicamente revisionate allo scopo di verificare che i permessi e le autorizzazioni di accesso siano sempre aggiornate.
	Assegnazione dei privilegi	L'assegnazione dei privilegi agli operatori deve avvenire in base al principio del "need-to-know" e della "segregation of duties".
	Password policy	Le password di accesso degli operatori incaricati dell'assistenza devono essere composte da almeno dodici (12) caratteri, prevedere caratteri alfanumerici e caratteri speciali, essere sostituite almeno ogni novanta (90) giorni, qualora si tratti di utenze privilegiate nella configurazione del SW, e conservate in formato crittografato.
	Utilizzo della VPN	L'erogazione del servizio di assistenza e di accesso alla piattaforma da remoto devono avvenire mediante connessione VPN con MFA. La VPN può essere del Cliente o configurata dalla SWH in accordo col Cliente; prima dell'utilizzo di ogni sessione ci deve essere l'autorizzazione del Cliente che deve attivare o disattivare l'accesso ai propri sistemi in relazione alle attività svolte e richieste dallo stesso. Al termine dell'intervento l'operatore di assistenza dovrà



		comunicare al Cliente la fine dell'intervento e richiedere la disattivazione dell'accesso.
Gestione Sicurezza Logica	Patch Management	Continuo patching applicativo di sicurezza relativo alla piattaforma per l'erogazione del supporto da remoto.
Log Management	Monitoraggio e gestione dei log di attività	Le attività svolte dagli operatori con utenze privilegiate devono essere tracciate e monitorate.
Supporto da remoto in modalità attended (con presidio di un soggetto autorizzato da parte del Cliente)	Gestione dell'escalation interna	Gli operatori incaricati dell'assistenza devono accertarsi che le richieste di assistenza provengano da un soggetto identificato e preventivamente autorizzato dal Cliente (ad esempio tramite autenticazione sulla piattaforma di ticketing).
	Gestione del sistema di supporto	Gli operatori incaricati dell'assistenza devono richiedere al Cliente in modo tracciabile le autorizzazioni necessarie ai fini dell'erogazione del servizio di assistenza (ad esempio, la condivisione dello schermo, il controllo condiviso dell'applicativo, il trasferimento dei file e la registrazione delle attività).
Supporto da remoto in modalità unattended	Assegnazione dei privilegi da parte del Cliente	Deve essere garantita al Cliente la possibilità di assegnare specifici diritti ai determinati operatori incaricati dell'assistenza al fine di limitare l'accesso ai propri sistemi solo al personale autorizzato e per un intervallo temporale definito.



Supporto da remoto in modalità unattended	Accesso al DB	L'accesso agli ambienti di produzione da parte di Utenti che non operano in qualità di amministratori di sistema è consentito unicamente in presenza di comprovate esigenze di assistenza/manutenzione e mediante un processo autorizzativo ad hoc che consenta di tracciare la richiesta/autorizzazione del Cliente (es. "trouble ticketing").
Attività di test	Utilizzo dei dati per l'esecuzione dei test	Utilizzo di dati fittizi (non dati reali) per l'esecuzione dei test. Solo in casi particolari, su richiesta del Cliente, ed in particolare quando sono sviluppate funzioni particolarmente complesse che devono essere provate e che devono essere verificate sull'esattezza della singola elaborazione e del singolo interessato presente negli archivi, prima di utilizzare gli archivi viene verificata l'adozione delle misure di sicurezza presenti negli ambienti di produzione. In questi casi i dati devono essere conservati per il tempo strettamente necessario all'esecuzione dell'attività di verifica della qualità e poi cancellati.



	Accesso agli ambienti dei Clienti tramite IP pubblici	Il collegamento tramite IP pubblici su ambienti cloud dovrà avvenire da parte degli operatori incaricati dell'assistenza con utenze individuali, che dovranno essere attivate dal Cliente al fine di evadere la richiesta di assistenza. Solo nel caso in cui è previsto un servizio di assistenza continuativo tali credenziali potranno rimanere sempre attive, ma in questo caso gli accessi degli operatori dovranno essere loggati e l'operatore per ogni intervento dovrà giustificare la finalità per cui l'ha dovuto effettuare. Per tale finalità l'ambiente applicativo potrà prevedere utenze precaricate a sistema e le procedure di assegnazione delle stesse saranno in carico alla SWH in relazione alle esigenze segnalate dal Cliente.
Gestione archivi	Autorizzazione per copia/trasferimento dati temporanei	L'eventuale copia o trasferimento di archivi o base dati del Cliente per finalità di assistenza o manutenzione deve essere preventivamente ed espressamente autorizzata dal Cliente stesso.
	Secure disposal	I DB/archivi del Cliente devono essere conservati per il tempo strettamente necessario all'esecuzione dell'attività di assistenza e immediatamente cancellati qualora non più necessari per l'esecuzione delle operazioni di assistenza.



		Le copie dei DB/archivi del Cliente prelevati per finalità di assistenza devono essere trasferite tramite canali sicuri e protetti, salvate in ambienti dotati delle opportune misure di sicurezza e non devono essere sottoposti a backup allo scopo di minimizzare il trattamento.
	Secure disposal	Qualora durante le attività di assistenza fosse necessario stampare documenti o informazioni, tali documenti devono rimanere nell'esclusiva disponibilità dell'operatore e da questi devono essere protetti contro accessi non autorizzati. Al termine dell'attività, i documenti dovranno essere distrutti.



	Attività migrazione conversione	In relazione alle attività di migrazione dei dati sono da prevedere le seguenti misure di sicurezza: - Utilizzo di canali sicuri e protetti nella trasmissione dei dati; - Utilizzo delle basi dati contenenti dati effettivi in ambiente dedicato, dotato di misure di sicurezza idonee a garantire la riservatezza; - Configurazione dei profili di accesso a tali ambienti al solo personale preposto dalla SWH alla gestione delle attività di migrazione compreso il test ed il collaudo. Ove richiesto, tali profili sono estesi anche al personale del Cliente. Qualora presenti, gli accessi da remoto avvengono sempre mediante l'utilizzo di canali sicuri; - Conservazione dei dati esclusivamente fino al buon fine del completamento delle attività di verifica ed alla conseguente consegna, approvazione e accettazione da parte del Cliente.
--	--	---



Governance	Tracciabilità	Sono adottati processi e strumenti di assistenza che assicurino la tracciabilità degli interventi richiesti ed eseguiti (piattaforma di ticketing).
Governance	Data Breach	Sono adottate procedure di gestione degli incidenti che consentono di individuare, contenere e risolvere situazioni di rischio (e.g. violazioni di dati personali) per la sicurezza dei dati e dei sistemi in fase post-intrusione.

In cloud

Il gestionale è utilizzato dal cliente

- tramite il data center della swh
- tramite data center esterni di sub fornitori della swh ma gestiti amministrativamente dalla stessa.
- Se il servizio è erogato da **data center esterni** che assumono la gestione sistemistica dei server e della infrastruttura per l'erogazione dei servizi la swh **vincola contrattualmente e verifica il subfornitore.**



Ambito	Catalogazione	Requisito di dettaglio
Misure sicurezza Data Center	Accesso al Sistema o SW (autenticazione)	Adozione di misure dirette a garantire che: - gli accessi di amministrazione da parte della SWH siano riservati al personale a cui sia attribuita la qualifica ("ruolo") di amministratore di sistema, in virtù di elevate capacità tecniche e caratteristiche di comprovata affidabilità e moralità; - l'accesso amministrativo ai sistemi da parte del personale del Cliente avverrà attraverso procedure di autenticazione a più fattori (MFA).



Misure sicurezza Data Center	Accesso al Sistema o SW (policy di gestione)	Per i servizi che prevedono una modalità di gestione amministrativa delle componenti infrastrutturali, devono essere previste le seguenti policy: - utenze che consentano l'individuazione dell'amministratore che esegue l'intervento; - attivazione di un processo di log management che identifichi i log in, log out e log in failed; - conservazione dei log in un formato che ne garantisca l'integrità e la lettura nel tempo; - conservazione dei log per almeno sei (6) mesi; - verifica annuale dell'operato degli amministratori di sistema; - accesso ai sistemi attraverso VPN e MFA.
Misure sicurezza Data Center	Log Management	Funzionalità per il tracciamento o registrazione (log) degli accessi e delle attività svolte dagli Utenti. I log concernenti le attività svolte devono essere opportunamente protetti a garanzia della loro integrità e riservatezza. Tali funzionalità devono essere attivabili da parte dell'amministratore di sistema del Cliente o della Software House su richiesta del Cliente.



Misure sicurezza Data Center	Auditing	Utilizzo del sistema di gestione e analisi dei log anche per il monitoraggio delle attività degli amministratori di sistema. L'accesso al sistema di gestione dei log è riservato al personale avente ruolo di auditor e non è ammesso per il personale addetto all'amministrazione di sistema.
Misure sicurezza Data Center	Crittografia dei protocolli di comunicazione	Applicazione di protocolli crittografici standard di comunicazione sicuri e non obsoleti, nei casi in cui l'accesso al sistema sia effettuato tramite Internet.
Misure sicurezza Data Center	Minacce e Vulnerabilità	Adozione di un programma di gestione delle minacce e dei rischi per monitorare continuamente le vulnerabilità delle Piattaforme SaaS indicate da best practice internazionali attraverso la pianificazione e l'esecuzione di scansioni delle vulnerabilità interne ed esterne e test di penetrazione. Le vulnerabilità identificate devono essere valutate per determinare i rischi associati e le opportune azioni correttive stabilite in base alla priorità assegnata e gravità rilevata.
Misure sicurezza Data Center	Firewalling	Adozione di sistemi di firewall finalizzati a filtrare e contenere il traffico identificando eventuale traffico anomalo indicatore di possibili attacchi informatici. Presenza di firewall L4 o L7/WAF.
Misure sicurezza Data Center	Intrusion Prevention	Protezione dell'ambiente mediante cui è erogato il servizio dalla SWH mediante Intrusion Prevention System (IPS) che permettono di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso. Il traffico di rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito.



Misure Center	sicurezza	Data	Malware protection	Adozione di misure di protezione da infezioni di software malevolo, di difesa da azioni non autorizzate, da applicazioni sospette e di protezione da tentativi di sottrazione di dati personali (es. mediante sistemi antivirus, antispyware, antiphishing, etc., mantenuti costantemente aggiornati).
Misure Center	sicurezza	Data	Filesystem Antivirus	Adozione di moduli Antivirus sul filesystem su tutti i server utilizzati per la fornitura dei servizi, con possibilità di configurare, su base progettuale, prodotti antivirus specifici gestiti centralmente in termini di aggiornamento, distribuzione delle policy, avvio di scansioni on demand, notifiche e gestione della area di quarantena.
Misure Center	sicurezza	Data	Monitoraggio e gestione incidenti	Adozione di policy e procedure per l'identificazione, gli interventi, i rimedi e le segnalazioni di incidenti che determinano un rischio per l'integrità o riservatezza dei dati personali o altre violazioni della sicurezza.
Misure Center	sicurezza	Data	Security Patch Management	Sottoposizione della piattaforma ad un processo periodico di verifica delle patch o delle fix disponibili relativamente alle componenti dell'impianto di erogazione e a quelle ritenute critiche per l'erogazione del servizio o per la sicurezza.
Misure Center	sicurezza	Data	Sicurezza fisica	Applicazione di adeguate misure di sicurezza fisica alla piattaforma hardware/software progettata (es. utilizzo di hosting provider/servizi di data center dotati di adeguati sistemi di prevenzione del rischio intrusione, incendio, allagamento, ecc.).



Misure Center	sicurezza	Data	Anti allagamento	Adozione nell'ambito del Data Center di tutte le misure necessarie a prevenire allagamenti (quali presenza di sonde, impianti di allarme, ecc.).
Misure Center	sicurezza	Data	Anti intrusione	Impostazione nel Data Center di un sistema di controllo degli accessi che identifichi coloro che accedono e impedisca l'accesso ai non autorizzati. La procedura deve prevedere anche la gestione del Change con l'attivazione e disattivazione dell'autorizzazione all'accesso in funzione dei cambi di ruolo.
Misure Center	sicurezza	Data	Telecamere a circuito chiuso	Installazione di telecamere (CCTV) per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche..
Misure Center	sicurezza	Data	Condizionamento	Adozione di adeguati impianti di condizionamento e di raffreddamento degli ambienti ed apparati.
Misure Center	sicurezza	Data	Continuità ed emergenza	Adozione di procedure e controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema/SW (in caso di incidente / violazione di dati personali). Le procedure devono comprendere le indicazioni per la conservazione delle copie di backup nonché un piano per il disaster recovery.
Misure Center	sicurezza	Data	Cancellazione dei dati	Previsione di misure per la cancellazione dei dati di produzione al termine dell'erogazione del servizio secondo i termini contrattuali definiti con il Cliente.
Misure center esterni	sicurezza	Data	Verifica dei requisiti del sub-fornitore e contrattualizzazione degli obblighi relativi alle misure di sicurezza	Selezione e verifica dei requisiti del sub-fornitore che assume la gestione sistemistica dei server e dell'infrastruttura necessari allo svolgimento dei



		Servizi e sottoscrizione di un contratto che vincoli il medesimo sub-fornitore al rispetto degli obblighi concernenti le misure di sicurezza (previsti dalla SWH per la gestione del DC).
Misure sicurezza Data center esterni	Audit nei confronti del sub-fornitore	Sottoposizione del sub-fornitore che gestisce il DC esterno ad audit periodici per la verifica del rispetto degli obblighi concernenti le misure di sicurezza, fatto salvo quanto previsto dalle condizioni di servizio fissate da providers multinazionali di servizi di DC ai sensi dell'art. 7.7 del CoC.
Connettività	Linee Internet e disponibilità di banda	Previsione di misure volte ad assicurare una connettività adeguata in conformità ai livelli di servizio contrattualmente definiti con il Cliente.
Connettività	Firewalling	Protezione dell'accesso ai sistemi contro il rischio d'intrusione attraverso adeguate misure di firewalling.
Sicurezza rete	AntiDDoS	Erogazione da parte del Data Center di un servizio in grado di rispondere in modo efficace alle problematiche create dagli attacchi ("DDoS").
Sicurezza rete	IDS/IPS	Adozione di un sistema IPS (Intrusion Prevention System) in grado di bloccare automaticamente gli attacchi rilevati e IDS (Intrusion Detection System) in grado di intercettare le minacce fornendo così una protezione real-time ai servizi erogati dal Data Center.
Governance	Formazione	Erogazione periodica di corsi di formazione sulla sicurezza e protezione dei dati personali ai propri dipendenti coinvolti nelle attività di trattamento.



Governance	Ubicazione geografica	Dichiarazione da parte della SWH nei confronti del Cliente dell'ubicazione geografica del DC e dei dati.
Governance	Data Breach	Adozione di procedure di individuazione, contenimento e risoluzione di situazioni di rischio (e.g. violazioni di dati personali) per la sicurezza dei dati e dei sistemi in fase post-intrusione.
Requisiti sistemistici e di gestione	Sicurezza logica	Rivalutazione con cadenza almeno annuale delle misure e procedure di sicurezza applicate in modo da aggiornarle in relazione alle vulnerabilità rilevate, agli attacchi subiti e all'evoluzione della tecnologia.

Altri obblighi della SwH Responsabile

Rendere l'informativa

Tenere il registro

Clienti: Rinvio a schede o db anagrafiche

Categorie trattamenti: Rinvio a documenti

Se Sub Responsabile

Solo indicazione del
cliente Responsabile + DPA

Analisi dei rischi - Valutazioni di impatto

Restano a carico del cliente (salve quelle necessarie alla SwH per il proprio adeguamento).

Ma la SwH **coadiuva il cliente** nei suoi assessment.

- Tramite il DPA
- gli allegati A e B
- altre certificazioni e documenti disponibili





Misure di sicurezza del software

Gli aggiornamenti non possono diminuire i livelli di sicurezza.

Non è dovuta la protezione delle infrastrutture e dei sistemi del cliente.

E' necessario fornire informazioni al cliente perché valuti in autonomia la rispondenza del sw alle proprie esigenze.



Incidenti di sicurezza

Procedura documentata per la gestione

Azioni da intraprendere

Persone da coinvolgere

Comunicazione al Cliente entro 48 ore

Pretendere lo stesso dai subfornitori

Personale della Software House

Riservatezza

Need to know

Istruzioni dettagliate

Formazione ripetuta e documentata

Diritti degli interessati

Dotare il SW di funzionalità per l'esercizio

Diritti 15 - 22 del Gdpr

Assistere il cliente

Definire chi risponde in caso di ricezione

Trasferimenti extra SEE

Se previsti (anche via sub Fornitori)

Paesi dichiarati adeguati

Garanzie Gdpr (artt. 44 ss.)

Accordo con il cliente

Preventiva informazione



Tempi di conservazione dati clienti

Secondo quanto previsto in contratto

Al termine: cancellazione

Tiene solo necessari ex lege

30 gg post cessazione per
consentire recupero al
cliente



Informazioni e verifiche del cliente

Fornire informazioni per adeguamento cliente

Consentire verifiche

Audit indipendenti (standard es.
ISO/IEC - OWASP)

Audit interni (documentati) con
previsioni di riservatezza e
segreto





Codice di condotta sw gestionali © 2024 by Andrea Broglia is licensed under CC BY-NC-ND 4.0.

Questa documentazione è sottoposta alla licenza sul diritto d'autore Creative Commons CC BY-NC-ND.

E' permessa la redistribuzione solo in forma intera e invariata, citando espressamente l'autore.

Non può essere modificata o distribuita commercialmente.

Qualsiasi utilizzo diverso potrà essere fatto solo se autorizzato espressamente dall'autore.



“

Gli androidi sognano pecore elettriche?

Philip K. Dick



Andrea Broglia Avvocato
info@studiolegalebrogli.com



CIPP/E Certified Information Privacy Professional | **DPO** UNI 11697:2017 | **A/LA** ISO IEC 27001:2022 | **A/LA** ISO IEC 42001:2023



BROGLIA
ANDREA
AVVOCATO