Misure tecniche ed organizzative - MTO

Allegato C al DPA - Data Protection Agreement

Ai sensi dell'art. 28 del Regolamento UE 2016/679 - GDPR

Versione 3.0 - 13/11/2026

dunp

sede legale: largo nino franchellucci, 61 - 00155 roma
p.i. e c.f. 09884631004 - cciaa rm 1195595

sede operativa: via giuseppe rosaccio, 6 - 00156 roma
T +3906.4066184 - F +3906.41220142
amministrazione@dunp.it - info@dunp.it - www.dunp.it

ISO 14001:2015 UNI 11506:2021 UNI 301549:2021 UNI 11621-3:2021 UNI/PdR 125:2022

1. Finalità del documento

Il presente documento descrive le principali Misure Tecniche e Organizzative (“MTO”) adottate da dunp s.c.p.l., in qualità di Responsabile del trattamento, per la protezione dei dati personali trattati per conto dei propri Clienti.

Le misure sono definite secondo un approccio proporzionato al rischio e tengono conto della natura del servizio, delle caratteristiche dell'infrastruttura utilizzata, delle categorie di dati trattati e delle istruzioni ricevute dal Titolare.

Il presente documento costituisce parte della documentazione collegata al DPA dunp v2.0.

Le misure descritte rappresentano il quadro generale applicabile ai servizi gestiti da dunp. Alcune misure possono non risultare tecnicamente applicabili a tutti i servizi o possono dipendere dal Profilo di Trattamento, dal provider utilizzato e dal livello di servizio specificamente acquistato dal Cliente.

2. Modello di responsabilità

dunp distingue tra:

- **misure direttamente implementate o gestite da dunp**, relative alle proprie attività applicative, sistemistiche e organizzative;
- **misure infrastrutturali**, implementate dai provider Cloud, Hosting e altri Sub-responsabili utilizzati;
- **misure di competenza del Cliente**, relative, ad esempio, alla gestione dei propri utenti, dispositivi, credenziali e istruzioni di trattamento.

Il livello di sicurezza complessivo deriva dall'insieme di tali misure.

L'utilizzo di infrastrutture di terzi non trasferisce automaticamente al provider le responsabilità proprie di dunp, né rende dunp responsabile delle componenti infrastrutturali non rientranti nel proprio controllo.

3. Controllo degli accessi e autorizzazioni

3.1 Accesso riservato al personale autorizzato

Gli accessi amministrativi e sistemistici ai sistemi gestiti da dunp sono riservati a personale espressamente autorizzato. dunp applica criteri di necessità e minimo privilegio, limitando l'accesso alle risorse effettivamente necessarie per lo svolgimento delle attività assegnate.

3.2 Account e privilegi

Ove tecnicamente possibile:

- vengono utilizzati account individuali;
- i privilegi amministrativi sono limitati;
- gli accessi non più necessari vengono revocati o modificati;
- le credenziali amministrative non devono essere condivise con soggetti non autorizzati.

3.3 Autenticazione multi-fattore

Per gli account utilizzati dal personale dunp per l'amministrazione delle infrastrutture VPS gestite è adottata autenticazione a due fattori, ove supportata dalla relativa piattaforma di gestione.

L'estensione della MFA agli utenti applicativi del Cliente dipende invece dalle funzionalità della piattaforma e dalle specifiche concordate nel progetto.

3.4 Accesso alle postazioni - Google Credential Provider for Windows (GCPW)

Le postazioni Windows aziendali abilitate utilizzano Google Credential Provider for Windows (GCPW), che consente al personale autorizzato di accedere al sistema operativo mediante le proprie credenziali Google Workspace.

Il sistema favorisce l'utilizzo di account individuali, l'applicazione delle politiche aziendali di autenticazione e la gestione centralizzata delle identità, contribuendo a ridurre il rischio di accessi non autorizzati.

3.5 Verifica della sicurezza dei dispositivi - Google Endpoint Verification

dunp utilizza Google Endpoint Verification per verificare informazioni tecniche e di sicurezza dei dispositivi che accedono alle risorse aziendali. Le verifiche possono comprendere identificativi del dispositivo, sistema operativo, stato di cifratura, presenza di protezioni per l'accesso e altre informazioni tecniche disponibili.

Le informazioni sono utilizzate per valutare le condizioni di sicurezza degli accessi e individuare eventuali configurazioni non conformi alle politiche aziendali.

3.6 Gestione centralizzata del browser - Google Chrome

dunp utilizza funzionalità di gestione centralizzata di Google Chrome per applicare politiche di sicurezza ai browser e ai profili di lavoro aziendali. Le misure possono comprendere la gestione delle estensioni, delle impostazioni di sicurezza, delle autorizzazioni e delle modalità di accesso alle risorse aziendali.

Sui dispositivi personali utilizzati per attività lavorative, la gestione è limitata al profilo Chrome aziendale, ove configurato esclusivamente a livello di profilo, mantenendolo separato dai profili personali.

4. Gestione delle credenziali e dei segreti

Password, API key, token, certificati, chiavi private e altre credenziali tecniche sono trattati come informazioni riservate. dunp adotta misure volte a limitarne l'accesso al personale autorizzato e a evitarne l'esposizione non necessaria.
Per attività automatizzate, ove tecnicamente previsto, vengono utilizzate credenziali o chiavi dedicate anziché account personali.

4.1 Gestione centralizzata delle credenziali – Passbolt Vault

dunp utilizza Passbolt Vault quale sistema centralizzato per la custodia e la condivisione sicura delle credenziali aziendali. Il sistema consente di organizzare password e credenziali tecniche, assegnare autorizzazioni individuali e limitarne la disponibilità al personale incaricato. L'utilizzo del Vault contribuisce a ridurre la condivisione di password attraverso canali non protetti e favorisce una gestione controllata degli accessi ai sistemi aziendali e dei Clienti.

5. Protezione delle comunicazioni

Le applicazioni web gestite da dunp utilizzano, ove tecnicamente applicabile, connessioni HTTPS/TLS per la protezione dei dati durante la trasmissione.

I certificati digitali necessari all'erogazione dei servizi vengono configurati e mantenuti nell'ambito delle attività tecniche previste.

Gli accessi amministrativi vengono effettuati mediante protocolli appropriati alla piattaforma e all'infrastruttura utilizzata.

6. Sicurezza delle infrastrutture server

Le infrastrutture direttamente gestite da dunp possono essere protette mediante una combinazione delle seguenti misure:

- firewall;
- sistemi di controllo e filtraggio del traffico;
- Web Application Firewall o sistemi equivalenti;
- ModSecurity ove disponibile;
- regole di filtraggio delle richieste web;
- limitazione degli accessi amministrativi;
- logging tecnico;
- strumenti di sicurezza messi a disposizione dal provider;
- aggiornamenti di sistema e componenti amministrati.

Le caratteristiche tecniche effettivamente disponibili dipendono dal provider e dal piano infrastrutturale utilizzato.

7. Protezione degli accessi ai database

I database gestiti da dunp non vengono, ove possibile, resi liberamente accessibili da Internet. L'accesso remoto viene limitato alle esigenze tecniche effettivamente necessarie e può essere sottoposto a:

- regole firewall;
- allowlist IP;
- restrizioni di rete;
- autenticazione;
- ulteriori controlli previsti dall'infrastruttura.

Qualora sia necessario concedere accesso a sistemi di terzi indicati dal Cliente, l'abilitazione viene configurata in funzione della specifica integrazione richiesta.

8. Sicurezza applicativa

Per siti, portali, e-commerce, CRM e applicazioni sviluppate o gestite da dunp vengono adottate, in funzione dell'architettura e del servizio acquistato, misure quali:

- autenticazione degli utenti;
- gestione di ruoli e permessi;
- protezione delle sessioni;
- comunicazioni HTTPS;
- validazione degli input;
- gestione controllata degli errori;
- protezione delle aree amministrative;
- logging tecnico;
- aggiornamento dei componenti gestiti;
- limitazione dell'esposizione non necessaria di informazioni tecniche.

Per form pubblici possono essere utilizzati meccanismi anti-abuso o anti-bot quali Google reCAPTCHA o strumenti equivalenti (honey-pot) in funzione delle caratteristiche del progetto.

9. Ciclo di sviluppo software digitali

Per software e piattaforme sviluppati da dunp vengono adottate misure proporzionate alla complessità del progetto e al livello di rischio.

Ove applicabile ciò include:

- utilizzo di ambienti di sviluppo e produzione distinti;
- gestione controllata del codice;
- repository di versionamento;
- test prima del rilascio;
- gestione delle dipendenze;
- limitazione dell'uso di dati personali reali negli ambienti di sviluppo quando non necessario;
- procedure di pubblicazione e aggiornamento.

Quando l'accesso a dati reali è necessario per troubleshooting, manutenzione o debugging, esso viene limitato alle attività strettamente necessarie.

10. Aggiornamenti e patch

dunp gestisce gli aggiornamenti e le patch relative alle componenti comprese nel servizio acquistato, tenendo conto di:

- criticità della vulnerabilità;
- disponibilità della correzione;
- compatibilità con l'applicazione;
- rischi connessi all'aggiornamento;
- perimetro del contratto di manutenzione.
- Importante: esclusioni dal servizio standard

Salvo specifica previsione contrattuale, il servizio standard non costituisce un servizio continuativo di managed security o vulnerability management e non comprende automaticamente:

- scansioni programmate di vulnerabilità;
- security review periodiche;
- SLA specifici di patch management;

- SOC/SIEM;
- remediation continuativa;
- vulnerability assessment formali;
- penetration test;
- code review di sicurezza periodiche.

11. Logging

Le infrastrutture e applicazioni gestite possono produrre log relativi, tra l'altro, a:

- richieste HTTP/HTTPS;
- errori del web server;
- anomalie applicative;
- autenticazioni;
- eventi tecnici;
- eventi riconducibili a sistemi di protezione quali ModSecurity;
- attività amministrative ove supportate dalla piattaforma.

I log sono utilizzati per diagnostica, troubleshooting, sicurezza, analisi degli incidenti e gestione tecnica del servizio. L'accesso ai log è riservato ai soggetti autorizzati. La tipologia e la durata dei log dipendono dal servizio, dal sistema operativo, dall'applicazione e dal provider utilizzato.

11.1 Registri di controllo e audit - Google Workspace

dunp utilizza le funzionalità di registrazione, controllo e audit disponibili nella Console di amministrazione Google Workspace per verificare eventi amministrativi, accessi e attività rilevanti per la sicurezza delle risorse aziendali.

In funzione delle funzionalità disponibili, dell'edizione Google Workspace e delle configurazioni adottate, i controlli possono comprendere:

- **Autenticazioni e accessi:** accessi riusciti e non riusciti, eventi sospetti e informazioni tecniche relative alle sessioni.
- **Sicurezza degli account:** modifiche delle password, configurazione della verifica in due passaggi e attività relative al recupero degli account.
- **Attività amministrative:** modifiche alle impostazioni di sicurezza, agli utenti, ai ruoli, ai privilegi e alle configurazioni dei servizi.

- **Applicazioni e autorizzazioni:** concessione e revoca di autorizzazioni OAuth, utilizzo di applicazioni di terze parti e accessi federati SAML.
- **Google Drive:** eventi relativi a creazione, modifica, eliminazione, accesso e condivisione dei file, nei limiti della registrazione disponibile.
- **Gmail:** eventi tecnici e di sicurezza relativi alla posta elettronica, ove supportati dall'edizione e dagli strumenti di audit disponibili.
- **Dispositivi:** registrazione e gestione degli endpoint, variazioni dello stato di sicurezza e accessi alle risorse aziendali.
- **Google Chrome:** eventi di sicurezza, configurazioni e informazioni relative ai browser o ai profili gestiti, ove disponibili.

I registri sono utilizzati per finalità di sicurezza, verifica delle configurazioni, individuazione di anomalie, analisi degli incidenti e protezione delle informazioni aziendali e dei Clienti.

L'accesso ai registri è riservato agli amministratori espressamente autorizzati.

La disponibilità, la granularità e i tempi di conservazione degli eventi dipendono dalle funzionalità e dalle politiche di conservazione applicabili.

12. Monitoraggio delle disponibilità

Per i servizi soggetti a monitoraggio, dunp utilizza strumenti automatizzati per verificare la raggiungibilità delle piattaforme e rilevare indisponibilità tecniche. Tra gli strumenti utilizzati da dunp rientrano servizi di uptime monitoring, anche attraverso UptimeRobot/Nootify.
Il monitoraggio della raggiungibilità:

- non equivale a un SOC;
- non costituisce monitoraggio continuativo di tutti gli eventi di sicurezza;
- non garantisce l'assenza di incidenti;
- non modifica gli SLA contrattualmente applicabili.

13. Backup

Per i servizi nei quali è prevista la gestione del backup, dunp utilizza procedure di copia dei dati proporzionate alla configurazione infrastrutturale.

Le strategie possono includere:

- snapshot del server;
- backup incrementali;
- copie su infrastruttura distinta da quella primaria;
- copie ulteriori di sicurezza;
- procedure di ripristino.

La frequenza, la retention e il numero delle copie applicabili al singolo servizio sono eventualmente definiti da apposito accordo contrattuale.

14. Separazione delle copie di backup

Ove previsto dall'architettura, dunp mantiene almeno una copia dei dati su infrastruttura o ambiente distinto dalla produzione. L'uso di provider o ambienti distinti contribuisce alla riduzione del rischio di perdita derivante dall'indisponibilità del sistema principale.

L'eventuale utilizzo di Sub-responsabili per backup e storage è riportato nel Registro dei Sub-responsabili dunp.

15. Ripristino

Le procedure di backup sono finalizzate a consentire, nei limiti della configurazione adottata, il ripristino dei sistemi e dei dati. Il semplice servizio di backup non equivale ad un servizio completo di Disaster Recovery.

16. Disaster Recovery, RPO e RTO

Salvo espressa previsione nel Preventivo o in uno specifico Addendum, i servizi standard dunp non comprendono:

- infrastrutture di Disaster Recovery dedicate;
- replica geografica in alta disponibilità;
- RPO contrattualmente garantiti;
- RTO contrattualmente garantiti;
- test periodici di Disaster Recovery;
- backup immutabili;
- procedure di failover automatico.

Eventuali esigenze specifiche devono essere oggetto di analisi, progettazione e quotazione.

17. Sicurezza delle postazioni dunp

Le postazioni utilizzate dal personale autorizzato per attività amministrative e tecniche sono protette mediante misure coerenti con il rischio.

Tali misure comprendono o possono comprendere, in funzione della postazione e del sistema:

- autenticazione individuale;
- blocco dell'accesso;
- gestione mediante identità aziendale;
- aggiornamento del sistema operativo;
- strumenti anti-malware;
- controllo degli accessi;
- protezione delle credenziali.

17.1 Monitoraggio della sicurezza degli endpoint aziendali - SIEM

dunp ha introdotto un sistema centralizzato di monitoraggio della sicurezza informatica (SIEM - Security Information and Event Management), applicato alle postazioni e ai sistemi aziendali inclusi nel relativo perimetro.

La piattaforma consente, in funzione degli agenti installati e delle funzionalità abilitate, di raccogliere e analizzare eventi di sicurezza, rilevare configurazioni potenzialmente rischiose, individuare vulnerabilità conosciute e segnalare anomalie o possibili minacce.

Le verifiche possono comprendere lo stato delle configurazioni di sicurezza, l'inventario tecnico dei sistemi, gli eventi di autenticazione, le anomalie di sistema e le modifiche rilevanti ai componenti monitorati.

Il sistema supporta le attività di prevenzione, analisi e risposta agli incidenti, senza sostituire le ulteriori misure di protezione adottate.

18. Sicurezza fisica e data center

Per i sistemi Cloud/VPS, le misure fisiche dei data center sono affidate ai provider infrastrutturali indicati nel Registro dei Sub-responsabili. Esse possono comprendere, secondo la documentazione del provider:

- controllo degli accessi fisici;
- presidio delle infrastrutture;
- ridondanza;
- continuità elettrica;
- prevenzione incendi;
- monitoraggio ambientale;
- sicurezza perimetrale.

dunp non attribuisce a sé certificazioni possedute esclusivamente dai provider utilizzati.

19. Sicurezza fisica e data center

Nella selezione e gestione dei provider infrastrutturali possono essere considerate certificazioni, attestazioni e standard di sicurezza messi a disposizione dagli stessi. Tali certificazioni sono riferibili esclusivamente al soggetto certificato e ai relativi servizi o infrastrutture e non si intendono automaticamente estese a dunp.

Le informazioni aggiornate sui provider e sulle relative garanzie possono essere rese disponibili al Cliente su richiesta o tramite la documentazione ufficiale del provider.

20. Cifratura a riposo (dati at-rest)

La disponibilità e configurazione della cifratura dei dati a riposo dipende dall'infrastruttura, dal provider e dal servizio utilizzato. Ove richiesta come requisito specifico del progetto, la cifratura at-rest deve essere verificata nell'ambito della relativa configurazione tecnica.

21. Gestione degli incidenti

dunp dispone di una procedura interna documentata per la gestione delle violazioni di dati personali e degli eventi di sicurezza, nonché di un registro interno degli eventi. La procedura disciplina:

- rilevazione e raccolta delle informazioni;
- analisi e classificazione;
- contenimento e gestione;
- eventuale escalation;
- documentazione dell'evento;
- valutazione dell'eventuale coinvolgimento di dati personali.

21.1 Integrazione degli eventi di sicurezza

Le informazioni provenienti dai sistemi di monitoraggio, dai registri Google Workspace e dagli strumenti di sicurezza degli endpoint possono essere utilizzate dagli amministratori autorizzati per ricostruire eventi anomali, individuare possibili incidenti e definire gli interventi di contenimento e remediation necessari.

Gli eventi rilevanti sono gestiti secondo le procedure interne di sicurezza e, qualora coinvolgano dati personali trattati per conto dei Clienti, secondo le disposizioni applicabili del DPA.

22. Data Breach

Qualora dunp venga a conoscenza di una violazione di dati personali relativa a dati trattati per conto di un Cliente, informa il Titolare senza ingiustificato ritardo, secondo quanto previsto dal DPA dunp. La comunicazione viene integrata progressivamente con le informazioni disponibili.

La valutazione circa l'eventuale notifica all'Autorità di controllo o comunicazione agli interessati rimane di competenza del Titolare, fatti salvi gli obblighi direttamente applicabili a dunp.

23. Gestione di anomalie e tentativi di attacco

Eventi anomali, traffico sospetto, tentativi di accesso o altre evidenze rilevate tramite log e sistemi tecnici possono essere analizzati e, ove necessario, mitigati mediante:

- blocco di IP;
- aggiornamento delle regole firewall;
- modifica delle configurazioni;
- restrizione degli accessi;
- ulteriori interventi tecnici appropriati.

Non ogni evento di sicurezza costituisce automaticamente una violazione di dati personali.

24. Sub-responsabili

dunp può affidare alcune componenti del trattamento a Sub-responsabili che forniscono garanzie adeguate in termini di sicurezza e protezione dei dati.

I provider applicabili sono individuati nell' Allegato B – Registro dei Sub-responsabili: https://www.dunp.it/sub-responsabili.pdf

Le misure infrastrutturali implementate dai provider costituiscono parte del modello complessivo di sicurezza del servizio.

25. Servizi e integrazioni scelti dal Cliente

Qualora il Cliente richieda l'integrazione con servizi, piattaforme o soggetti terzi non incaricati da dunp, dunp configura l'integrazione secondo le istruzioni ricevute ma ciò non determina automaticamente l'assunzione del ruolo di Sub-responsabile da parte del soggetto terzo rispetto a dunp. La qualificazione privacy del rapporto tra il Cliente e il fornitore da esso scelto resta di competenza del Cliente, salvo diversa configurazione contrattuale.

26. Vulnerability Assessment e Penetration Test

Vulnerability Assessment, Penetration Test, code review specialistiche, security audit indipendenti e verifiche analoghe costituiscono servizi specialistici separati, salvo che siano espressamente inclusi nel Preventivo. Possono essere:

- effettuati da dunp ove rientrino nelle proprie competenze;
- affidati a soggetti specializzati;
- eseguiti da soggetti incaricati direttamente dal Cliente.

I risultati possono determinare l'adozione di ulteriori misure di remediation.

27. Misure aggiuntive in funzione del rischio

Qualora il livello di rischio di uno specifico progetto lo richieda, possono essere concordate:

- MFA obbligatoria per gli utenti amministrativi dell'applicazione;
- revisione periodica degli account;
- vulnerability assessment / penetration test;
- vulnerability management;
- policy di patch management;
- cifratura at-rest;
- backup immutabili;
- versioning / restore test periodici
- definizione formale di RPO e RTO;
- alerting di sicurezza;
- monitoraggio avanzato SOC/SIEM;
- segregazione aggiuntiva;
- ulteriori misure risultanti da una DPIA.

28. Riesame delle misure

dunp adotta un approccio di miglioramento continuo e può aggiornare le misure tecniche e organizzative in funzione di:

- evoluzione tecnologica;
- vulnerabilità e nuovi rischi;
- incidenti;
- modifiche dell'infrastruttura;
- nuovi servizi e/o evoluzione normativa;
- richieste dei Titolari;
- risultanze di audit o valutazioni di sicurezza.

Le misure possono essere sostituite con soluzioni equivalenti o superiori purché il livello complessivo di protezione non venga sostanzialmente ridotto.

29. Responsabilità del Cliente

Il Cliente mantiene la responsabilità delle misure rientranti nel proprio ambito di controllo. A titolo esemplificativo:

- individuazione degli utenti autorizzati;
- custodia delle credenziali;
- revoca degli accessi non più necessari;
- sicurezza dei propri dispositivi;
- corretto utilizzo della piattaforma;
- gestione dei propri fornitori;
- comunicazione a dunp di requisiti di sicurezza specifici;
- comunicazione della presenza di categorie particolari di dati o trattamenti ad alto rischio.

30. Livello di servizio e delimitazione del perimetro

Le MTO descritte nel presente documento non ampliano il perimetro tecnico o economico dei servizi acquistati dal Cliente.

In particolare, la presenza nel presente documento di una possibile misura di sicurezza non implica che siano automaticamente inclusi: SOC, SIEM, penetration testing, vulnerability management, Disaster Recovery, alta disponibilità, RTO/RPO garantiti o altre attività specialistiche, salvo esplicita previsione contrattuale.

30.1 Distinzione tra misure interne e servizi di sicurezza ai Clienti

Gli strumenti GCPW, Google Endpoint Verification, Google Chrome gestito, Passbolt Vault e SIEM rientrano nelle misure di sicurezza adottate da dunp per la protezione del proprio ambiente informatico e delle attività svolte per conto dei Clienti.

La loro adozione non comporta automaticamente l'erogazione di servizi dedicati di monitoraggio della sicurezza, SOC, SIEM, vulnerability management o gestione degli endpoint sulle infrastrutture dei Clienti, che rimangono soggetti a specifica previsione contrattuale.

Il Responsabile dunp scpl

(Timbro e Firma)

