# Politiche aziendali sull'utilizzo dei dispositivi personali nel posto di lavoro; uso, accesso privilegiato alle informazioni aziendali e loro applicazioni in Compilance GDPR

Approvato con delibera n.14 del 03/03/2021 del Commissario Straordinario facente funzioni di Consiglio di Istituto

| | |
|---|---|
| **Titolare del Trattamento** | Istituto Onnicomprensivo di Borgorose |
| **Codice Meccanografico** | RIIC81900A |
| **Indirizzo** | Via Micangeli, 41 - 02021 Borgorose (RI) |
| **Codice Fiscale** | 90033720575 |
| **e-mail** | riic81900a@istruzione.it |
| **PEC** | riic81900a@pec.istruzione.it |
| **Dirigente scolastico** | MARCELLO FERRI |
| **DPO** | APPIERTO CLAUDIA |

| Edizione | Revisione | Data | Descrizione | il Titolare | il DPO |
|---|---|---|---|---|---|
| 1 | 0 | 15/01/2021 | Prima emissione | *approvato* | *verificato* |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Documento di nr 30 pagine compresa la presente realizzato su format della**

# 1. Premessa

**Bring your own device (BYOD)**, in italiano: *porta il tuo dispositivo* - è un'espressione usata per riferirsi alle politiche aziendali che permettono di portare i propri dispositivi personali nel posto di lavoro, e usarli per avere gli accessi privilegiati alle informazioni aziendali e alle loro applicazioni.
Il BYOD consente la containerizzazione, vale a dire creare due ambienti diversi sullo stesso dispositivo, con dati aziendali e dati personali (chiamate, SMS, localizzazione GPS, ecc) rigorosamente separati, fin ad avere una Virtual Machine a livello del Sistema Operativo controllata dall'IT aziendale, o nel firmware del processore (a livello hardware, al di sotto del sistema operativo), o ricorrere a soluzioni di hosted virtual desktop (HVD) o virtual mobile OS, con cui l'utente si collega alla Intranet aziendale ad applicazioni e dati che fisicamente risiedono su un server remoto.
Il termine è anche usato per descrivere le stesse pratiche applicati agli studenti che usano i loro dispositivi in ambito educativo.

## 1.1. Vantaggi del BYOD

Un vantaggio ovvio tangibile che un'azienda ottiene adottando politiche BYOD è rappresentato dalla riduzione dei costi. Considerando poi una naturale propensione a utilizzare con più diligenza un oggetti di proprietà piuttosto che quelli forniti da altri, si può ipotizzare una eventuale riduzione dei costi di riparazione.
Anche per i dipendenti non mancano i vantaggi: possono scegliere di utilizzare il dispositivo con cui si sentono più a loro agio e che conoscono già. Il lavoro sui propri strumenti IT, di conseguenza, agevola l'approccio del dipendente al lavoro diminuendo lo stress lavoro-correlato e portando un aumento della sua produttività.
Lavorare su strumenti personali significa utilizzare dispositivi mobili; in questo modo i dipendenti ottengono completa flessibilità: i dati aziendali diventano reperibili in ogni momento e in ogni luogo. È possibile quindi lavorare in ufficio come a casa e nei tempi che si desidera. Se un dipendente non termina il lavoro quotidiano in ufficio, ad esempio, può sempre portare a termine il lavoro da casa. Questo, unito ai vantaggi precedenti, fa si che un'organizzazione che utilizza politiche BYOD incrementa la produttività dei suoi impiegati e diventa più attraente per coloro che sono in cerca di lavoro.

## 1.2. Svantaggi del BYOD

Anche se la possibilità di consentire al personale di lavorare in qualsiasi momento da qualsiasi luogo e su qualsiasi dispositivo offre vantaggi reali, porta anche rischi significativi. È fondamentale per l'azienda mettere in atto misure di sicurezza per proteggere dati, servizi e informazioni sensibili.
È possibile che un dipendente perda o divulghi dati aziendali a causa di negligenza, imperizia, colpa, colpa grave o dolo.
Esempio: se un dipendente utilizza il suo smartphone per accedere alla rete aziendale e perde il telefono, chiunque lo trova potrebbe leggere e utilizzare i dati presenti sul dispositivo. O, ancora, se un impiegato vende il suo tablet o il suo smartphone senza una corretta pulizia del contenuto, cede tutte le informazioni a cui aveva accesso ad un utente sconosciuto.
Un altro tipo di violazione della sicurezza si verifica quando un dipendente chiude il rapporto di lavoro senza restituire i suoi dispositivi o senza una corretta pulizia degli stessi: in questo caso le applicazioni aziendali e altri dati rimangono accessibili anche se non lo dovrebbero più essere.
Consideriamo in ultimo il caso in cui un dispositivo sia dato in mano ai famigliari del dipendente: può capitare che i bambini che giocano con questi strumenti pubblichino involontariamente delle informazioni riservate ivi contenute.

# 2. Introduzione

Quando il personale aziendale (c.d. "*incaricato al trattamento dei dati personali*") utilizza dispositivi mobili personali per le sue esigenze operative, può elaborare dati personali di terzi (c.d. "*interessati*") su tali dispositivi. In queste situazioni, è l'azienda (c.d. "*titolare del trattamento dei dati personali*") che ha la responsabilità di garantire il rispetto dei principi di protezione dei dati, in particolare del regolamento 2016/679 (c.d., "*il regolamento*" o "GDPR") al fine di garantire i diritti alla privacy e alla protezione dei dati personali, indipendentemente dalla fornitura o meno dei dispositivi mobili.

La presente politica aziendale e la relativa procedura operativa sono rivolte ai Responsabili del trattamento, al DPO e a tutti gli incaricati, nonché al personale IT e di sicurezza IT e ad altri servizi amministrativi interessati ai processi relativi all'uso professionale dei dispositivi mobili.
La politica aziendale e la procedura operativa forniscono un'analisi dei rischi di protezione dei dati relativi al trattamento dei dati personali su dispositivi mobili, nonché istruzioni e procedure operative (c.d. "*best practices*") per il raggiungimento di un livello di protezione dei dati conforme al regolamento. L'applicazione costante delle istruzioni e delle procedure operative da parte di tutti gli incaricati contribuiscono alla validazione della corretta valutazione e susseguente mitigazione dei rischi connessi al trattamento dei dati personali. L'elenco delle azioni e delle misure consigliate in queste linee guida non intende essere esaustivo o esclusivo in quanto le stesse saranno periodicamente monitorate e, se del caso, aggiornate o modificate.

## 2.1. Background tecnico

I dispositivi mobili, in particolare smartphone e tablet, pervadono la vita professionale e privata. Ora sono "*dispositivi informatici generici*" che eseguono quasi tutte le applicazioni. Oltre alle chiamate vocali e ai messaggi di testo, offrono la possibilità di utilizzare servizi Internet (social network, condivisione di contenuti, ecc.) e dispongono di molti sensori che forniscono una quantità crescente di informazioni collegate ai propri utenti, come la posizione e un numero crescente di parametri ambientali e personali.
I dispositivi mobili intelligenti hanno avuto un profondo impatto sul modo in cui lavorano le organizzazioni. Si stanno sviluppando sempre più applicazioni per questi dispositivi che stanno sostituendo workstation e laptop per alcuni usi. Tra i vantaggi vi sono l'aumento della soddisfazione dei dipendenti, il risparmio sui costi e la capacità di soddisfare le crescenti esigenze di mobilità.
Smartphone e tablet non sono gli unici dispositivi mobili utilizzato nelle organizzazioni: anche l'archiviazione portatile, come schede di memoria, chiavette USB e dischi rigidi, ha avuto un grande impatto sull'archiviazione, la trasmissione e la sicurezza dei dati. **I rischi per la sicurezza e la privacy impliciti nel loro utilizzo sono elevati e non sono trascurati dal Titolare.**
A tal proposito sono state individuate diverse criticità:

- gli utenti di dispositivi mobili per motivi di lavoro (incaricati) potrebbero trattare dati personali senza essere consapevoli che un'azione sul dispositivo mobile potrebbe comportare un trattamento di dati personali che è soggetto alle condizioni e ai limiti del Regolamento. Il Titolare è consapevole del fatto che, poiché le operazioni di trattamento dei dati eseguite dagli incaricati nell'esercizio delle loro funzioni sono attribuibili al Titolare, rimane responsabile di queste operazioni di trattamento, anche se le operazioni potrebbero essere solo "transazionali" (ad es. inoltrare una e-mail con i dati di contatto di un nuovo collega);
- i dispositivi mobili consentono l'utilizzo di applicazioni software che interagiscono con le risorse web. Si scambiano informazioni tramite le loro interfacce di rete a volte senza che gli utenti o le istituzioni ne siano consapevoli;
- quando gli incaricati utilizzano i propri dispositivi privati per scopi professionali (ad esempio, l'accesso e l'archiviazione di informazioni informatiche) vengono sollevati ulteriori problemi di protezione dei dati in quanto utilizzano lo stesso dispositivo per comunicazioni personali e per altri scopi con app di loro scelta. Il Titolare non può esercitare lo stesso livello di verifica e controllo sui dispositivi privati che ha con i dispositivi di proprietà istituzionale.

Pertanto, il principio di responsabilizzazione è di fondamentale importanza nel contesto dell'uso dei dispositivi mobili. Ciò è particolarmente importante a causa della complessità di definire chiaramente le responsabilità specifiche di ogni attore coinvolto in base ai molteplici casi d'uso possibili.

# 3. Ambito, metodologia e struttura

## 3.1. Scopo

La presente politica aziendale e la relativa procedura operativa forniscono disposizione contrattuale sul rispetto delle norme sulla privacy e sulla protezione dei dati nel contesto dell'uso di dispositivi mobili da parte degli incaricati per scopi professionali. La presente non pregiudica politiche separate o specifiche che il Titolare possa prendere in considerazione o in relazione ad altri fini istituzionali.
La presente politica aziendale e la relativa procedura operativa riguardano sia i dispositivi mobili forniti dal Titolare sia quelli di proprietà degli incaricati se utilizzati per scopi professionali (BYOD). Il termine "*dispositivi mobili*" comprende:

- ✓ telefoni,
- ✓ smartphone,
- ✓ tablet,
- ✓ laptop, notebook e netbook,

ovvero

- ✓ tutti i dispositivi che consentono al personale di lavorare in mobilità, nonché dispositivi di archiviazione come dischi rigidi esterni e unità flash USB.

Questi dispositivi presentano rischi comuni a causa del loro aspetto "mobile" e delle dimensioni ridotte, sebbene le misure di sicurezza che possono essere implementate, pertanto l'obiettivo principale del presente documento è fornire istruzioni per quanto riguarda l'uso di smartphone e tablet. Per altri dispositivi mobili si applicano i sottoinsiemi dei rischi e le misure indicate.
Sebbene l'uso di dispositivi mobili per scopi professionali sollevi generalmente molti problemi di sicurezza informatica, i rischi relativi alle risorse informative appartenenti al Titolare rientrano nell'ambito di applicazione di questi orientamenti solo nella misura in cui i rischi informatici hanno un impatto sui dati personali.
La politica aziendale e la sua relativa procedura operativa affrontano le seguenti problematiche:

- principi generali per il trattamento dei dati personali tramite dispositivi mobili da parte del Titolare;
- rischi per i dati personali elaborati con dispositivi mobili;
- best practices per proteggere i dati personali.

Poiché l'uso del dispositivo mobile da parte di un incaricato per i suoi scopi personali non è un trattamento effettuato da o per conto del Titolare non rientra nell'ambito di applicazione del Regolamento non vengono affrontati i seguenti scenari e argomenti:

- incaricati che utilizzano dispositivi di proprietà del Titolare per scopi personali (anche se **vietato**);
- gli incaricati che utilizzano esclusivamente a scopo personale dispositivi mobili privati (anche se portati sul luogo di lavoro);
- i rischi per gli interessi e i beni del Titolare diversi da quelli relativi alla protezione dei dati personali (es. protezione della proprietà intellettuale o informazioni classificate);
- l'elaborazione di dati di comunicazioni elettroniche per il rilevamento dell'uso non autorizzato di dispositivi mobili;
- le analisi su dispositivi mobili degli incaricati da parte del Titolare o della magistratura nel contesto di indagini.

## 3.2. Metodologia

Il processo decisionale che ha portato alla stesura e approvazione del presente documento è stato concepito in modo che siano il risultato di un dialogo aperto e strutturato tra Titolare, Responsabile e incaricati. Gli elementi principali di questo processo sono:

- l'esercizio di accertamento dei fatti per raccogliere fatti e raggiungere una migliore comprensione della posizione del Titolare in materia;
- l'elaborazione dei risultati dell'indagine di cui al punto precedente;
- la revisione delle best practices sulla sicurezza dei dispositivi mobili;
- la finalizzazione del documento.

Questo documento viene rivisto annualmente e eventualmente aggiornato e revisionato.

### 3.3. Struttura

Questo documento è strutturato come segue:

a) **Istruzioni operative:** presenta l'elenco delle istruzioni da attuare sulla base degli obblighi previsti dal regolamento. Il contenuto di questa sezione è il più rilevante sia per i DPO che per il personale di sicurezza IT del Titolare in quanto specifica il contenuto che una "*politica dei dispositivi mobili*" dovrebbe avere.

b) **Misure di sicurezza:** per proteggere i dati personali trattati con dispositivi mobili utilizzando best practices per affrontare i rischi associati ai dispositivi mobili.

c) **Problemi di protezione dei dati:** relativamente al trattamento dei dati personali tramite dispositivi mobili discute in modo più dettagliato le diverse questioni legali relative all'uso dei dispositivi mobili definiti nell'ambito di questo documento.

d) **Rischi:** per i dati personali trattati da dispositivi mobili descrive alcuni dei rischi associati ai dispositivi mobili.

## 4. Istruzioni operative

Questa sezione contiene una serie di istruzioni operative che aiuteranno il Titolare a dimostrare la conformità al Regolamento durante il trattamento dei dati personali tramite dispositivi mobili. Queste istruzioni devono essere interpretate come i diversi componenti di un criterio per i dispositivi mobili secondo il diagramma seguente:

| Policy per l'utilizzo di dispositivi mobili | | |
|---|---|---|
| **Titolare e DPO (R1)** | **Analisi costi / benefici (R2)** | **Uso accettabile della policy (R3)** |
| **Valutazione d'impatto sulla protezione dei dati (R4)** | **Risk Management (R5)** | **Data Breach (R6)** |
| **BYOD (R7)** | **Rettifica, blocco o cancellazione (R8)** | **Notifica al Garante (R9)** |

## 4.1. R1: Titolare e DPO

Il DPO è coinvolto riguardo a tutti gli aspetti dell'introduzione e dell'uso dei dispositivi mobili. (vedi sezione V.1)

## 4.2. R2: Analisi costi / benefici

È effettuata una valutazione caso per caso dei vantaggi di consentire l'uso di dispositivi mobili per specifiche operazioni di trattamento tenendo conto dei rischi e dell'invasività che tale uso può comportare (vedi sezione V.1).

## 4.3. R3: Uso accettabile della policy

Il Titolare adotta una *politica di utilizzo accettabile* per quanto riguarda i dispositivi mobili (vedi sezione V.1). Questa politica include anche gli obblighi dell'incaricato in merito al ciclo di vita dei dispositivi mobili.

## 4.4. R4: Valutazione d'impatto sulla protezione dei dati (DPIA)

È stata eseguita una DPIA sugli strumenti di monitoraggio e controllo utilizzati per garantire la sicurezza dei dispositivi mobili. Questa DPIA affronta i principali principi e norme sulla protezione dei dati di cui al Regolamento, tra cui:

- legalità,
- necessità e proporzionalità,
- specifica e limitazione dello scopo e delle finalità,
- qualità dei dati,
- conservazione dei dati,
- informazioni agli interessati e diritti degli interessati (accesso, rettifica, cancellazione, blocco),
- trasferimenti di dati e riservatezza delle reti di telecomunicazioni interne o delle apparecchiature terminali.

(vedi sezione V.3)

## 4.5. R5: Risk Management

Il Titolare dispone di un processo di gestione dei rischi adeguatamente documentato: i Responsabili del trattamento e gli incaricati adottano misure tecniche e organizzative appropriate per salvaguardare l'uso sicuro dei dispositivi mobili. Queste misure garantiscono un livello di sicurezza adeguato al rischio presentato, tenendo conto delle soluzioni tecniche disponibili e del costo della loro implementazione (vedi sezione V.2).

## 4.6. R6: Data Breach

Vengono adottate procedure interne per la gestione delle violazioni dei dati, compresa la notifica da parte del Titolare al Garante (vedi sezione V.4).

## 4.7. R7: BYOD

Quando il BYOD è consentito, il Titolare:

- valuta i rischi per i dati personali istituzionali e privati prima di introdurre BYOD nell'organizzazione (vedi sezione V.2).
- applica una politica che disciplina il BYOD. (vedi sezione V.1).

### 4.8. R8: Rettifica, blocco o cancellazione

Nel caso in cui siano presenti copie locali di dati personali su dispositivi mobili, è anche essenziale che i dati personali memorizzati sul dispositivo mobile siano anche oggetto di rettifica, blocco o cancellazione quando l'interessato esercita il diritto di rettificare i dati personali inesatti o incompleti o il diritto di bloccare o cancellare i dati trattati illecitamente. (vedi sezione V.5).

### 4.9. R9: Notifica al Garante

L'uso di dispositivi mobili in quanto tali non è, in linea di principio, un motivo per sottoporre le operazioni di trattamento al controllo preventivo del Garante (vedi sezione V.1). La necessità di sottoporre un trattamento a un'operazione di trattamento al controllo preventivo del Garante è analizzata alla luce delle "*finalità*" del trattamento.

## 5. Misure di sicurezza per proteggere i dati personali trattati nei dispositivi mobili

Questa sezione fornisce un elenco delle misure di sicurezza tecniche e organizzative quale requisito contrattuale al fine del trattamento dei dati personali. Questo elenco è periodicamente valutato , se necessario, aggiornato o modificato adottando misure integrative o alternative per soddisfare le esigenze specifiche del Titolare sulla base della propria valutazione dei rischi e del livello di sicurezza necessario. Il diagramma seguente riassume queste misure di sicurezza:

| Misure di Sicurezza | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Organizzative | | | | Tecniche | | | | | |
| Ciclo di vita del Dispositivo Mobile | Politica di sicurezza delle informazioni | Formazione / Sensibilizzazione | BYOD | Gestione dei Dispositivi Mobili (MDM) | | | Altre | | |
| | | | | Violazioni della sicurezza / incidenti di sicurezza | Risorse | Software | Crittografia Pseudo - nimizzazione | Controllo accessi | Sicurezza fisica |

### 5.1. Misure organizzative

L'introduzione di dispositivi mobili in un'organizzazione richiede la definizione di una politica globale che includa processi, piani di formazione, coinvolgimento della direzione e procedure per affrontare incidenti come violazioni dei dati.

#### 5.1.1. Gestione del ciclo di vita del dispositivo mobile

Il Titolare adottare procedure documentate per la gestione dell'intero ciclo di vita dei dispositivi mobili, dal suo acquisto (inventario), alle manutenzioni, fino alla sua dismissione.
Tali procedure coprono tutte le fasi rilevanti del ciclo di vita del dispositivo mobile - dall'acquisto allo smaltimento - tenendo conto di tutte le operazioni che devono essere eseguite sul dispositivo.
Nell'ambito di questa gestione del ciclo di vita, il Titolare ha configurato e mantiene un inventario dei dispositivi mobili che include, per ogni dispositivo, almeno:

- ✓ identificazione del dispositivo e, ove applicabile, identificazione della SIM;
- ✓ stato del dispositivo (es: nuovo, in manutenzione, assegnato, da smaltire…);
- ✓ utente a cui è allocato il dispositivo, con l'indicazione di inizio e di fine dell'assegnazione ove appropriato (es. dispositivi del pool allocati temporaneamente);
- ✓ proprietà (di proprietà istituzionale / BYOD).

Una politica di smaltimento delle risorse è particolarmente importante per i dispositivi mobili. Questa politica definisce gli obblighi degli incaricati. Inoltre, prevede la conservazione delle informazioni come parte dell'inventario completo dei dispositivi mobili sui dispositivi contrassegnati per lo smaltimento. La scelta dei metodi di smaltimento si basa sulla valutazione delle vulnerabilità di sicurezza associate a ciascun metodo di smaltimento e prevede che i dispositivi siano smaltiti in modo da garantire in particolare che tutti i dati personali siano cancellati nel caso in cui i dispositivi vengano rimossi.

### 5.1.2. Politica di sicurezza delle informazioni

Il Titolare adotta una politica sulla sicurezza delle informazioni e in particolare una politica sulla sicurezza dei dispositivi mobili, nonché la rispettiva informativa sulla privacy redatta in modo chiaro e completo. I responsabili della sicurezza e il DPO sono coinvolti nella redazione delle politiche di sicurezza e degli avvisi sulla privacy sin dalle prime fasi.

### 5.1.3. Formazione e Sensibilizzazione

Annualmente il Titolare effettua un'analisi dei fabbisogni formativi dei dipendenti ove stabilisce un piano di formazione per aumentare la consapevolezza degli incaricati su come proteggere i dati personali sui dispositivi mobili quando si consente il loro utilizzo.
Questo piano di formazione segue le politiche sui dispositivi mobili del Titolare e includere almeno i seguenti argomenti:

a) funzioni di base, sicurezza e privacy del dispositivo mobile;
b) applicazioni e servizi relativi alle imprese;
c) uso e sicurezza fuori sede (es. trasferte);
d) divieto di uso privato di dispositivi di proprietà istituzionale;
e) BYOD.

Il piano di formazione è annualmente valutato e aggiornato.
La formazione è obbligatoria come "corso di aggiornamento" per ogni incaricato che utilizza dispositivi mobili.

### 5.1.4. Misure organizzative per BYOD

Il Titolare, coadiuvato dal Resp. IT e dagli Amministratori di Sistema (se necessario), stabilisce i requisiti minimi applicabili ai BYOD per garantire che le politiche dell'organizzazione siano applicabili ai dispositivi (ad es. restrizioni sul tipo o sulla versione del dispositivo, sul tipo di sistema operativo, sulle configurazioni, sull'antivirus, ecc.).
Fornisce agli incaricati supporto tecnico per la configurazione dei dispositivi in linea con le politiche dei dispositivi mobili in materia di sicurezza, privacy e protezione dei dati.

### 5.1.5. Violazioni della sicurezza / incidenti di sicurezza

Le procedure di sicurezza prevedono una risposta pronta ed efficace a qualsiasi incidente di sicurezza (come lo smarrimento o il furto di un dispositivo mobile). Questi processi tengono conto dei requisiti di protezione dei dati e coinvolgono il DPO ad ogni incidente.
Gli incaricati al trattamento che utilizzano dispositivi mobili sono informati su come e dove segnalare incidenti di sicurezza come lo smarrimento o il furto del dispositivo. Particolare attenzione è prestata al fatto che gli utenti normalmente non saranno in ufficio al momento dell'incidente e quindi sono predisposti mezzi adeguati per la segnalazione di incidenti di sicurezza che coprano tutti gli scenari ragionevoli in cui un utente può trovarsi.

## 5.2. Misure tecniche

Esistono diversi rischi relativi al trattamento dei dati personali. La maggior parte delle volte la migliore, e anche l'unica, soluzione ad alcuni di questi problemi è l'attenta valutazione delle applicazioni installate su un dispositivo mobile e la corretta configurazione dei sistemi operativi nonché delle applicazioni.
La gestione e la configurazione dei dispositivi, dei sistemi operativi e delle applicazioni veniva tradizionalmente svolta da professionisti dedicati del reparto IT.

Con l'introduzione dei dispositivi mobili, spesso utilizzati come BYOD, alcune di queste attività vengono svolte direttamente dagli incaricati, con tutti i limiti di conoscenza e competenza in materia di security IT e privacy.
Per affrontare questa difficile situazione, il Titolare adotta due approcci:

1. aumenta la comprensione e la consapevolezza degli incaricati sui rischi per la protezione dei dati e sulle possibili contromisure attraverso il paino di formazione e sensibilizzazione;

e

2. utilizza adeguate soluzioni di "*gestione dei dispositivi mobili*" (MDM) che, come misure tecniche, soddisfano i requisiti di sicurezza e protezione dei dati.

### 5.2.1. Gestione dei dispositivi mobili (MDM)

Le soluzioni di gestione dei dispositivi mobili (MDM) sono utilizzate dal dipartimento IT del Titolare per eseguire determinate attività relative alla configurazione e alla gestione dei dispositivi mobili a fini di sicurezza. Tuttavia, questa capacità comporta maggiori responsabilità per il Titolare poiché questo tipo di software comporta un trattamento dei dati personali piuttosto intrusivo (ad esempio, l'MDM può consentire il monitoraggio dei dispositivi mobili in tempo reale). Il rispetto dei requisiti di protezione dei dati è quindi essenziale.
Il tipico set di funzionalità che una soluzione MDM include è:

- Sicurezza:
  - imporre l'uso della password del dispositivo per accedere al dispositivo mobile, ad applicazioni o contenitori specifici nonché alle chiavi private;
  - blocco e cancellazione da remoto del dispositivo (solo di tutti i dati sul dispositivo o delle informazioni istituzionali);
  - rilevamento del cambio di configurazione;
  - limitare l'accesso dell'utente e dell'applicazione all'hardware del dispositivo;
  - limitare l'accesso dell'utente e dell'applicazione ai servizi del sistema operativo nativo;
  - registri sicuri e audit-trail delle attività di gestione BYOD;
  - backup e ripristino delle informazioni istituzionali nel dispositivo mobile;
  - verifica della conformità prima di accedere alle risorse istituzionali;
  - crittografia dei dati sia a riposo (nel dispositivo) che in transito (crittografia delle comunicazioni);
  - distribuzione e gestione di certificati digitali.
- Gestione dei dispositivi:
  - applicazione centralizzata delle politiche di sicurezza;
  - distribuzione over-the-air (OTA) di software (applicazioni e aggiornamenti) e modifiche alle politiche.
- Gestione degli accessi:
  - blocco e cancellazione di applicazioni remote;
  - whitelist e blacklist delle applicazioni;
  - negozi di applicazioni aziendali;
  - distribuzione sicura delle applicazioni con controlli adeguati contro la manomissione;
  - inventario delle applicazioni per dispositivo (sia istituzionali che personali);
  - sicurezza delle applicazioni.

Non tutti i sistemi MDM potrebbero essere in grado di implementare queste funzionalità su tutti i possibili dispositivi mobili ma solo su un sottoinsieme. In questo caso il Responsabile IT segnala la mancanza al Titolare il quale la tiene in debita considerazione quando decide quali dispositivi mobili consentire.
In tutti i casi dove viene implementata una soluzione MDM, si adottano le seguenti misure:

- valutazione dell'impatto sulla protezione dei dati della soluzione MDM;
- informazione agli utenti tramite la politica di utilizzo accettabile dell'uso della soluzione MDM sul proprio dispositivo, del tipo di informazioni raccolte tramite MDM e dello scopo di questa raccolta;

- limitazione dell'accesso alla file system di amministrazione della soluzione MDM in base ai privilegi minimi, in base alle esigenze di conoscenza;
- valutazione della copertura della soluzione MDM rispetto all'inventario completo dei dispositivi mobili e ad altre fonti di informazioni come applicazioni o registri di rete.

### 5.2.2. Altre misure tecniche

Una soluzione MDM da sola non affronta tutti i rischi implicati dall'uso di dispositivi mobili. Il seguente elenco fornisce misure tecniche che sono previste, a seconda dei rischi specifici del Titolare. Alcune di queste misure traggono vantaggio da una soluzione MDM per la loro implementazione, sebbene non ne richieda una per essere funzionali. Queste misure di sicurezza sono prese in considerazione anche con dispositivi specifici: la crittografia può essere applicata alla memoria di archiviazione portatile, ad esempio chiavette USB, ma non software anti-malware, almeno nella chiavetta USB stessa.

1. Progettare, implementare e mantenere una soluzione di *sandboxing*, compartimentalizzazione o virtualizzazione per separare le informazioni private e istituzionali.
2. Sviluppare, implementare e testare una soluzione di crittografia che dovrebbe garantire che i dati personali archiviati sui dispositivi mobili (o, almeno, nel "compartimento istituzionale" del dispositivo, se è in uso una soluzione di compartimentazione / MDM) siano crittografati. Questa soluzione può contenere:
    - il requisito per la crittografia completa del disco per tutti i dispositivi e per la crittografia aggiuntiva per contenitori sicuri di applicazioni;
    - il requisito di utilizzare solo algoritmi di crittografia standard;
    - la lunghezza delle chiavi di crittografia scelte deve essere adeguata ai requisiti di sicurezza.
3. Sviluppare, implementare e testare una soluzione di backup per garantire la disponibilità delle informazioni archiviate solo nel dispositivo mobile.
4. Progettare e applicare un'autenticazione utente adeguata al dispositivo mobile, inclusi PIN e password per sbloccare il dispositivo mobile.
5. Disabilitare le funzionalità non necessarie.
6. Applicare una configurazione predefinita sicura e rispettosa della privacy per dispositivi mobili e applicazioni.
7. Garantire aggiornamenti software tempestivi del dispositivo mobile e delle applicazioni installate su di esso (utilizzando o meno una soluzione MDM).
8. L'accesso alle reti interne del Titolare è concesso solo dopo aver convalidato la connessione di rete da un dispositivo mobile contro l'elenco e le autorizzazioni istituzionali.
9. Consentire solo il traffico crittografato tra i dispositivi mobili e la rete interna del Titolare.
10. Utilizzare firewall standard del settore e applicazioni antimalware sui dispositivi mobili e bloccare l'accesso alla rete istituzionale ai dispositivi privi di tali firewall e applicazioni e / o con configurazioni obsolete. Sia il firewall che l'applicazione anti-malware devono essere aggiornati periodicamente, automaticamente o meno, tramite un file Soluzione MDM o direttamente con il fornitore del firewall o dell'applicazione anti-malware.
11. Secondo la politica di utilizzo, bloccare qualsiasi utilizzo di applicazioni di terze parti per elaborare i dati personali del Titolare, a meno che non sia previsto dalle politiche del Titolare e dopo un'adeguata valutazione incentrata sui rischi per i dati personali.

# 6. Problemi di protezione dei dati relativi al trattamento dei dati personali tramite dispositivi mobili

## 6.1. V.1 – Titolare del trattamento dati

Nell'ambito delle attività di trattamento svolte tramite dispositivi mobili è particolarmente importante sottolineare che per dato personale si intende qualsiasi informazione relativa a persona fisica identificata o identificabile: si tratta non solo di dati relativi al personale alle dipendenze del Titolare, ma anche di persone al di fuori di un rapporto di lavoro con il Titolare.

Il Titolare deve anche raccogliere e trattare ulteriormente i dati personali per la gestione dei dispositivi mobili stessi e spesso possono anche installare su di essi software ad hoc. È il caso dell'installazione delle cosiddette soluzioni "*Mobile Device Management*" (MDM), che aggiungono funzionalità per i dati relativi alla sicurezza, raccolta e interventi sui dispositivi, collegandoli a server centrali di controllo dedicati.
Quando un incaricato utilizza un dispositivo mobile per compiti legati al lavoro su istruzioni del Titolare, Il Titolare è responsabile dell'accaduto, sia in termini positivi che negativi, in quanto determina le finalità e i mezzi del trattamento dei dati personali. Il trattamento effettuato tramite dispositivo mobile rientra quindi nell'ambito di applicazione del Regolamento.
Anche nello scenario BYOD, più problematico di quello istituzionale a causa del ridotto controllo che il Titolare ha sul dispositivo mobile, il Titolare è comunque responsabile dell'adozione di tutte le misure necessarie per adempiere agli obblighi previsti dal Regolamento e per istituire il meccanismo interno per dimostrare tale conformità. Il Titolare non trascura che l'elaborazione tramite dispositivi mobili deve soddisfare gli stessi requisiti e principi delle operazioni di elaborazione nell'ambiente desktop "tradizionale".
**L'incaricato che utilizza il proprio dispositivo per lo svolgimento di compiti legati al lavoro (BYOD) ha l'obbligo contrattuale di attuare le politiche specificamente adottate dal Titolare per questo contesto.**
In linea con il principio di responsabilità, è importante che il DPO sia coinvolto sin dalle prime fasi della pianificazione e gestione del trattamento dei dati tramite dispositivi mobili per garantire che le misure adottate per mitigare o annullare i rischi per la protezione dei dati siano appropriate e conformi il regolamento.
I seguenti scenari sono, quindi, considerati i principali esempi di trattamento dei dati personali attraverso l'utilizzo di dispositivi mobili:

- il trattamento dei dati da parte degli incaricati tramite dispositivi mobili (da dispositivi di proprietà del Titolare o secondo lo scenario BYOD) come strumento per operazioni di elaborazione dati simili a quelle già svolte dal Titolare nell'IT tradizionale (di seguito, "*desktop*");
- il monitoraggio dell'utilizzo del dispositivo mobile dell'incaricato da parte del Titolare, nei limiti della legislazione applicabile;
- il trattamento dei dati personali nel contesto della distribuzione di soluzioni MDM.

In tutti i casi sopra indicati, si applica il Regolamento.
Il Regolamento stabilisce le condizioni alle quali il trattamento dei dati personali può essere lecito. **Il Titolare del trattamento garantisce che i membri del personale non utilizzino dispositivi mobili per elaborazioni non coperte da una base giuridica.**
La necessità e la proporzionalità del trattamento dei dati personali mediante dispositivi mobili richiede che il Titolare effettui una valutazione caso per caso dei vantaggi di tali strumenti rispetto ai rischi e all'invasività che il trattamento può comportare. Questa valutazione tiene conto delle funzionalità e delle caratteristiche aggiuntive del dispositivo mobile (come, ad esempio, l'arricchimento di un elenco di contatti con fotografie scattate con il dispositivo mobile).
Gli utenti dei dispositivi mobili (incaricati) sono informati del trattamento dei dati in corso a causa del loro utilizzo di dispositivi mobili, qualunque essi siano dispositivi di proprietà istituzionale o personali. Ancora di più quando i dati personali vengono raccolti e ulteriormente elaborati per la gestione dei dispositivi mobili stessi. Il Titolare adotta una politica di utilizzo accettabile per quanto riguarda i dispositivi mobili, che include:

- usi chiaramente definiti dei dispositivi mobili approvati dal Titolare,
- conseguenze dell'uso improprio delle risorse mobili,
- quali informazioni istituzionali e dati personali possono essere archiviati e trasferiti su dispositivi mobili,
- tipo e versione dei dispositivi mobili e dei sistemi operativi approvati,
- quali applicazioni possono essere installate e utilizzate,
- la politica del Titolare sull'uso dei servizi cloud,
- politica di restituzione e smaltimento,

- una chiara descrizione delle responsabilità dell'incaricato e del Titolare,
- a quali condizioni è consentito il monitoraggio dell'uso dei dispositivi mobili da parte degli incaricati,

e

- un avviso sui dati personali che l'incaricato può raccogliere ed elaborare tramite il proprio dispositivo mobile.

La politica di utilizzo accettabile deve essere formalmente accettata dagli incaricati prima che possano utilizzare i dispositivi mobili. Nel caso in cui la politica di utilizzo accettabile cambi, la nuova dovrà essere tempestivamente comunicata agli incaricati che dovranno accettarla nuovamente.
Per quanto riguarda lo scenario BYOD, la politica che disciplina il BYOD è facilmente disponibile per tutti i possibili utenti di BYOD (incaricati) prima che decidano di utilizzare o meno i propri dispositivi mobili per questioni professionali. Questa politica include la conformità "*opt-in*" alla politica, oltre alla politica di utilizzo accettabile per tutti i dispositivi mobili, come condizione per l'autorizzazione BYOD; e autorizzazione utente "*opt-in*" per la gestione dei sistemi e il monitoraggio dei dispositivi BYOD.
La configurazione del dispositivo mobile riflette le regole (anche in conformità ai principi di privacy by design e by default, e al principio di minimizzazione dei dati). Per quanto riguarda l'implementazione del principio di specificazione / limitazione delle finalità è evitato il "*creep delle funzioni*" (raccolta e trattamento dei dati per scopi secondari non consentiti), ad esempio escludendo l'installazione di app non necessarie per il lavoro-attività correlate e separare i dati del Titolare dai dati privati.

## 6.2. V.2 - Obbligo di sicurezza ai sensi del regolamento

Il titolare del trattamento adottare misure tecniche e organizzative adeguate per salvaguardare l'uso sicuro dei dispositivi mobili. Queste misure garantiscono un livello di sicurezza adeguato al rischio presentato, tenendo conto delle soluzioni tecniche disponibili e del costo della loro attuazione.
Ciò implica che il titolare del trattamento implementa un processo di gestione del rischio delle informazioni secondo principi di buona pratica stabiliti. Il primo passo di questo processo è la valutazione dei rischi, che include un'analisi dell'uso dei dispositivi mobili. Questa valutazione del rischio aiuta a determinare i principali rischi per la sicurezza e fornisce la base per selezionare i controlli appropriati che sono implementati per ridurre i rischi a un livello accettabile dalla direzione. Il processo di gestione del rischio include la revisione periodica della valutazione del rischio e dell'adeguatezza dei presidi e dei controlli.
Questo processo di gestione del rischio delle informazioni è adeguatamente documentato come politica del Titolare, è riesaminato regolarmente per garantire che rimanga efficace e in linea con obiettivi aziendali nuovi e in evoluzione. Gli incaricati e i Responsabili del trattamento che prendono parte al processo (in particolare all'analisi dei rischi per la sicurezza) sono coadiuvati da rappresentanti del lato "*core business*" (HR, core / attività operative) e dal DPO per garantire che l'analisi tenga conto dell'impatto su tutti gli aspetti dei trattamenti.

## 6.3. V.3 - Valutazione dell'impatto sulla protezione dei dati (DPIA)

### 6.3.1. Descrizione sistematica del trattamento

| Descrizione del trattamento | Finalità del trattamento | Legittimo interesse perseguito | |
|---|---|---|---|
| | | Non applicabile | Descrizione |
| Utilizzo di sistemi BYOD per attività lavorative | Finalità istituzionali, ivi comprese il flusso comunicativo dei dati (es. mail) | ☐ | Perseguimento finalità istituzionali |

#### 6.3.1.1. Natura, ambito di applicazione, contesto e finalità del trattamento

| | |
|---|---|
| **Natura del trattamento** | Dalla raccolta alla distruzione |
| **Ambito di applicazione** | Trattamento elettronico del dato personale con sistemi BYOD |
| **Contesto e finalità del trattamento** | Finalità istituzionali |
| **Fonti di rischio** | Rischi informatici tra cui perdita, distruzione o divulgazione non autorizzata |

| 1. Valutazione del rischio prima dell'applicazione delle misure di attenuazione | | | | |
|---|---|---|---|---|
| **Probabilità (P)** | | ☐ **BASSO (1)** | ☒ **MEDIO (2)** | ☐ **ALTO (3)** |
| **Gravità (G)** | | ☐ **BASSO (1)** | ☐ **MEDIO (2)** | ☒ **ALTO (3)** |
| **Rischio R = P x G** | **TOT.** | ☐ **BASSO (1-2)** | ☒ **MEDIO (3-7)** | ☐ **ALTO (8-9)** |
| | **6** | | | |

##### 6.3.1.1.1. Misure, garanzie e meccanismi previsti per attenuare il rischio MEDIO

| | |
|---|---|
| Rischi presentati dal trattamento a dati personali trasmessi, conservati o comunque trattati: | ☒ Distruzione<br>☒ Perdita<br>☒ Modifica<br>☒ Divulgazione non autorizzata<br>☒ Accesso |

| **Parametri considerati:** | | | | | | |
|---|---|---|---|---|---|---|
| Stato dell'arte | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Costi di attuazione | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Diritti e libertà delle persone fisiche | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

| | | |
|---|---|---|
| Adesione a codice di condotta approvato (art. 40)? | ☐ **SI** | ☒ **NO** |
| Meccanismo di certificazione approvato (art. 42)? | ☐ **SI** | ☒ **NO** |
| ***Se entrambe le risposte sono negative compilare la descrizione delle misure tecniche e organizzative.*** | | |

| **Misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio:** | | |
|---|---|---|
| **Misura** | **Descrizione** | |
| Pseudonimizzazione dei dati personali | ☐ **N.A.** | Effettuato quanto possibile nel file system |
| Cifratura dei dati personali | ☒ **N.A.** | |
| Capacità di assicurare su base permanente la riservatezza dei sistemi e dei servizi di trattamento | ☐ **N.A.** | Limitazione degli accessi, antivirus e firewall "centralizzati" |
| Capacità di assicurare su base permanente l'integrità dei sistemi e dei servizi di trattamento | ☐ **N.A.** | Procedura disaster recovery |
| Capacità di assicurare su base permanente la disponibilità dei sistemi e dei servizi di trattamento | ☐ **N.A.** | Procedura di backup |
| Capacità di assicurare su base permanente la resilienza dei sistemi e dei servizi di trattamento | ☐ **N.A.** | |
| Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico | ☐ **N.A.** | |
| Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative | ☐ **N.A.** | A campione direttamente dall'interessato |

| **Formazione e sensibilizzazione** |
|---|
| Chiunque agisce sotto l'autorità del titolare del trattamento e/o del responsabile del trattamento e che ha accesso a dati personali (***incaricato del trattamento***) è stato istruito in tal senso dal titolare del trattamento?<br>☒ **SI** ☐ **NO** |

| **2. Valutazione del rischio dopo l'applicazione delle misure di attenuazione** | | | | |
|---|---|---|---|---|
| **Probabilità (P)** | | ☒ **BASSO (1)** | ☐ **MEDIO (2)** | ☐ **ALTO (3)** |
| **Gravità (G)** | | ☐ **BASSO (1)** | ☒ **MEDIO (2)** | ☐ **ALTO (3)** |
| **Rischio R = P x G** | **TOT.** | ☒ **BASSO (1-2)** | ☐ **MEDIO (3-7)** | ☐ **ALTO (8-9)** |
| | **2** | | | |

| **Dopo l'applicazione delle misure di attenuazione:** | | |
|---|---|---|
| Il rischio è attenuato? | ☒ **SI** | ☐ **NO** |
| È assicurata la protezione dei dati personali? | ☒ **SI** | ☐ **NO** |
| È dimostrata la conformità al GDPR? | ☒ **SI** | ☐ **NO** |

### 6.3.2. Destinatari e periodo di conservazione

| **I dati personali, oggetto del presente trattamento sono:** | | |
|---|---|---|
| **Misura** | **Descrizione** | |
| Trasmessi a destinatari | ☐ **N.A.** | Destinatari istituzionali e/o interessati. |
| Oggetto di conservazione per un tempo prestabilito (time-life) | ☐ **N.A.** | Secondo quanto stabilito nelle informative di cui agli artt. 13 e 14 GDPR |
| Descrizione funzionale del trattamento | ☐ **N.A.** | |

### 6.3.3. Risorse

| **Le risorse sulle quali si basano i dati personali sono:** | | |
|---|---|---|
| **Misura** | **Descrizione** | |
| Hardware (comprese le reti) | ☐ **N.A.** | BYOD |
| Software | ☐ **N.A.** | SIGLA, Android, Apple IOS, Microsoft office, Open Office |
| Persone (descrizione delle funzioni o mansioni) | ☐ **N.A.** | Incaricati del trattamento |
| Canali Cartacei | ☒ **N.A.** | |
| Trasmissione cartacea | ☒ **N.A.** | |

| **Codici di condotta** |
|---|
| Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati (art. 40)? |
| ☐ **SI** ☒ **NO** |

### 6.3.4. Necessità e proporzionalità dei trattamenti

#### 6.3.4.1. Misure per garantire il rispetto al GDPR

##### 6.3.4.1.1. Proporzionalità e necessità

| **Finalità:** | | | | | | |
|---|---|---|---|---|---|---|
| Determinate | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Esplicite | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Legittime | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Trattati in modo compatibile con tali finalità | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Archiviazione nel pubblico interesse | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Ricerca scientifica o storica o a fini statistici | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

| **Liceità (almeno una condizione):** | | | |
|---|---|---|---|
| L'interessato esprime il consenso al trattamento dei propri dati personali per una o più specifiche finalità | ☒ **SI** | ☐ **NO** | ☐ **N.A.** |
| Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso | ☒ **SI** | ☐ **NO** | ☐ **N.A.** |
| Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento | ☒ **SI** | ☐ **NO** | ☐ **N.A.** |
| Il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica | ☐ **SI** | ☒ **NO** | ☐ **N.A.** |
| Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento | ☒ **SI** | ☐ **NO** | ☐ **N.A.** |
| Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore | ☒ **SI** | ☐ **NO** | ☐ **N.A.** |
| Il trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti (in tale caso la condizione sopra indicata è soddisfatta) | ☒ **SI** | ☐ **NO** | ☐ **N.A.** |

**Il trattamento è effettuato per una finalità diversa da quella per la quale i dati personali sono stati raccolti ovvero su un atto legislativo?**

☐ **SI** ☒ **NO**

**Se la risposta è SI, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, si valuta:**

| **Misura** | **Descrizione** | |
|---|---|---|
| Esiste un nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto | ☐ **N.A.** | |
| Il contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento, ne giustifica il trattamento | ☐ **N.A.** | |
| Sono trattate categorie particolari di dati personali (art. 9), oppure dati relativi a condanne penali e a reati (art. 10) | ☐ **N.A.** | |
| Sono valutate le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati | ☐ **N.A.** | |
| Esistono garanzie adeguate, come ad esempio cifratura o pseudonimizzazione | ☐ **N.A.** | |

| **Minimizzazione dei dati:** | | | |
|---|---|---|---|
| I dati personali sono adeguati rispetto alle finalità per le quali sono trattati? | ☒ **SI** | ☐ **NO** | ☐ **N.A.** |
| I dati personali sono pertinenti rispetto alle finalità per le quali sono trattati? | ☒ **SI** | ☐ **NO** | ☐ **N.A.** |
| I dati personali sono limitati a quanto necessario rispetto alle finalità per le quali sono trattati? | ☒ **SI** | ☐ **NO** | ☐ **N.A.** |

### 6.3.4.1.2. Misure che contribuiscono ai diritti degli interessati

| **Informazioni fornite all'interessato:** | | | | | | |
|---|---|---|---|---|---|---|
| È disponibile all'interessato un'informativa relativa al trattamento, redatta in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| L'informativa è fornita per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Una volta comprovata l'identità dell'interessato, se richiesto, le informazioni sono fornite oralmente. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22 compresi. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Se il titolare del trattamento dimostra che non è in grado di identificare l'interessato rifiuta di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22 compresi. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il titolare del trattamento soddisfa la richiesta dell'interessato fatta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il termine di trenta giorni può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste, informando l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Se l'interessato presenta la richiesta ai sensi degli articoli da 15 a 22 mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento: | | | | | | |
| a) addebita un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| b) rifiuta di soddisfare la richiesta. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| L'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta è del titolare del trattamento. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, richiede ulteriori informazioni necessarie per confermare l'identità dell'interessato. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

| **Informazioni fornite all'interessato:** | | | | | | |
|---|---|---|---|---|---|---|
| L'informativa contiene: | | | | | | |
| l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| i dati di contatto del responsabile della protezione dei dati, ove applicabile; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| le finalità del trattamento cui sono destinati i dati personali e la base giuridica del trattamento; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| il diritto di proporre reclamo a un'autorità di controllo; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e in tal caso informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente. | □ | **SI** | □ | **NO** | □ | **N.A.** |
| L'informativa non viene data se: | | | | | | |
| l'interessato dispone già delle informazioni; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1; | □ | **SI** | □ | **NO** | □ | **N.A.** |
| nella misura in cui l'obbligo di fornire l'informativa rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. | □ | **SI** | □ | **NO** | □ | **N.A.** |
| l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; | □ | **SI** | □ | **NO** | □ | **N.A.** |

| | | | | | | |
|---|---|---|---|---|---|---|
| qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| È garantito all'interessato il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: | | | | | | |
| le finalità del trattamento; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| le categorie di dati personali in questione; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| il diritto di proporre reclamo a un'autorità di controllo; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| l'esistenza di un processo decisionale automatizzato, compresa la profilazione e in tal caso informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il diritto di ottenere una copia dei propri dati personali oggetto del trattamento non deve ledere i diritti e le libertà altrui. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare cui li ha forniti qualora il trattamento si basi sul consenso o su un contratto; e il trattamento sia effettuato con mezzi automatizzati. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

| **Informazioni fornite all'interessato:** | | | | | | |
|---|---|---|---|---|---|---|
| L'esercizio del diritto relativamente alla portabilità dei dati lascia impregiudicato l'esercizio del diritto all'oblio nelle modalità stabilite all'articolo 17. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il diritto ad ottenere la portabilità dei propri dati personali non deve ledere i diritti e le libertà altrui. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: | | | | | | |
| i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| i dati personali sono stati trattati illecitamente; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| i dati personali devono essere cancellati per adempiere un obbligo legale cui è soggetto il titolare del trattamento; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il titolare del trattamento, che ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il titolare del trattamento non soddisfa la richiesta fatta dall'interessato di diritto all'oblio nella misura in cui il trattamento sia necessario: | | | | | | |
| per l'esercizio del diritto alla libertà di espressione e di informazione; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| per motivi di interesse pubblico nel settore della sanità pubblica; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

| **Informazioni fornite all'interessato:** | | | | | | |
|---|---|---|---|---|---|---|
| L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi: | | | | | | |
| l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Se il trattamento è limitato, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| L'interessato che ha ottenuto la limitazione del trattamento è informato dal titolare del trattamento prima che detta limitazione sia revocata. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione sulla base di tali disposizioni. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il diritto di opposizione è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

| **Informazioni fornite all'interessato:** | | | | | | |
|---|---|---|---|---|---|---|
| Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento: | | | | | | |
| tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| adotti tutte le misure richieste ai fini della sicurezza del trattamento; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| rispetti le condizioni imposte dal GDPR per ricorrere a un altro responsabile del trattamento; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| assista il titolare del trattamento nel garantire il rispetto degli obblighi relativi alla sicurezza del trattamento, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

| **Informazioni fornite all'interessato:** | | | | | | |
|---|---|---|---|---|---|---|
| Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| L'adesione da parte del responsabile del trattamento a un codice di condotta approvato o a un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare le garanzie sufficienti. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il contratto o altro atto giuridico tra titolare e responsabile del trattamento è stipulato in forma scritta, anche in formato elettronico. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| **Trattamenti internazionali:** | | | | | | |
| Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| In mancanza di una decisione della Commissione, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Possono costituire garanzie adeguate per i trattamenti internazionali senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo: | | | | | | |
| uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| le norme vincolanti d'impresa (art. 47); | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| le clausole tipo di protezione dei dati adottate dalla Commissione; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| un codice di condotta approvato, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

| | | | | | | |
|---|---|---|---|---|---|---|
| un meccanismo di certificazione approvato, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| In mancanza di una decisione di adeguatezza o di garanzie adeguate, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni: | | | | | | |
| l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| il trasferimento sia necessario per importanti motivi di interesse pubblico; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Se non è possibile basare il trasferimento su una disposizione dell'articolo 45 o 46, comprese le disposizioni sulle norme vincolanti d'impresa, e nessuna delle deroghe in specifiche situazioni a norma del primo comma del presente paragrafo è applicabile, il trasferimento verso un paese terzo o un'organizzazione internazionale sia ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. Il titolare del trattamento informa del trasferimento l'autorità di controllo. In aggiunta alla fornitura di informazioni di cui agli articoli 13 e 14, il titolare del trattamento informa l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

| **Trattamenti internazionali:** | | | | | | |
|---|---|---|---|---|---|---|
| Il titolare del trattamento o il responsabile del trattamento attesta nel registro dei trattamenti la valutazione e le garanzie adeguate per il trasferimento internazionale dei dati personali. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| **Consultazione preventiva:** | | | | | | |
| Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Al momento di consultare l'autorità di controllo, il titolare del trattamento comunica all'autorità di controllo ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale; le finalità e i mezzi del trattamento previsto; le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento; ove applicabile, i dati di contatto del titolare della protezione dei dati; la valutazione d'impatto sulla protezione dei dati; ogni altra informazione richiesta dall'autorità di controllo. | ☐ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

### 6.3.4.1.3. Gestione dei rischi per i diritti e le libertà degli interessati

| **Rischi per diritti e libertà degli interessati:** | | | | | | |
|---|---|---|---|---|---|---|
| Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione è preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si consulta l'autorità di controllo. | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Il titolare del trattamento effettua una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto verte, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al regolamento. | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |

| **Rischi per diritti e libertà degli interessati:** | | | | | | |
|---|---|---|---|---|---|---|
| Nella valutazione di impatto sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati. | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Nella valutazione di impatto si consulta il responsabile della protezione dei dati. | ☒ | **SI** | ☐ | **NO** | ☐ | **N.A.** |
| Nella valutazione di impatto si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno. | ☐ | **SI** | ☒ | **NO** | ☐ | **N.A.** |

## 6.4. V.4 - Comunicazione delle violazioni dei dati

Il Titolare del trattamento adottare procedure interne per la gestione della sicurezza e delle violazioni dei dati che prevedano in particolare la notifica del verificarsi di tali eventi da parte dei responsabili del trattamento al DPO (vedi procedura "*Costituzione Comitato Data-Breach*").

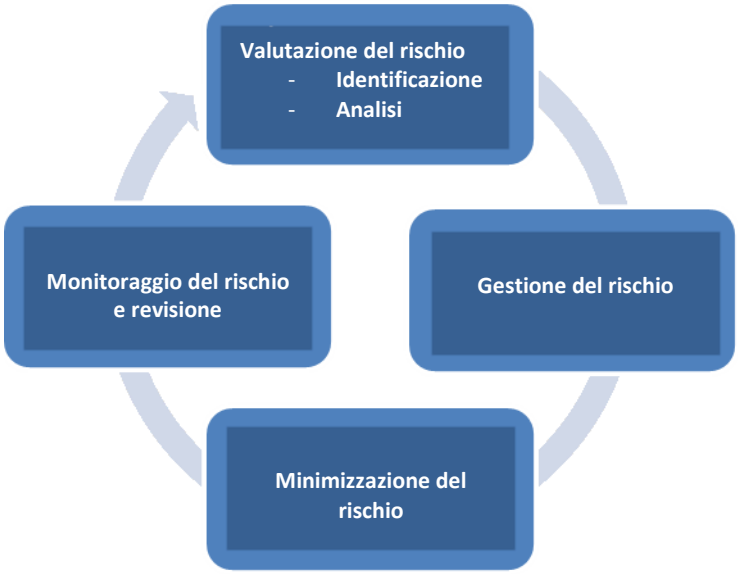
## 6.5. V.5 - Archiviazione secondaria dei dati personali tramite dispositivi mobili

Quando i dati personali vengono elaborati tramite un dispositivo mobile, l'incaricato potrebbe memorizzare copie dei dati personali dai sistemi informativi centrali sul dispositivo. Questa "*memorizzazione secondaria*" porta a problemi relativi alla qualità dei dati, all'esercizio dei diritti di rettifica, blocco e cancellazione da parte dell'interessato e per quanto riguarda il rispetto del periodo di conservazione dei dati pertinente.

Può accadere che questi dati memorizzati sul dispositivo mobile non siano accurati o mantenuti aggiornati, mentre i dati vengono aggiornati nel sistema di archiviazione centrale del Titolare. Per tale motivo la memorizzazione secondaria è considerata una prassi di trattamento dei dati sovraeccedente e il Titolare effettua formazione e sensibilizzazione agli incaricati per responsabilizzarli alla problematica.
Nel caso in cui le copie locali dei dati personali su dispositivi mobili facciano parte dell'operazione di trattamento come previsto dal Titolare, è anche essenziale che quando l'interessato eserciti il diritto di rettificare i dati personali che siano inesatti o incompleti o il diritto di bloccare o cancellare i dati trattati illecitamente, i dati personali memorizzati sul dispositivo mobile sono anche considerati per la rettifica, il blocco o la cancellazione.

# 7. Rischi per i dati personali trattati da dispositivi mobili

Questa sezione fornisce un elenco di rischi e minacce tipici per i dati personali nei dispositivi mobili, che sono presi in considerazione dal Titolare quando esegue la propria valutazione del rischio. Questo elenco fornisce una base per identificare i rischi e le minacce più importanti ed è oggetto di valutazione ed eventuale revisione periodica.
Come promemoria, nel diagramma successivo vengono presentate le componenti principali del processo di gestione del rischio.




I dispositivi mobili presentano maggiori rischi per i dati personali rispetto ai computer desktop a causa della loro portabilità e, nel caso di smartphone e tablet, della loro capacità di raccogliere e condividere grandi quantità di informazioni contestuali, della loro natura "*sempre attiva*", del loro numero e della diversità di sensori (ad esempio: GPS, bussola digitale, giroscopio, accelerometro, sensore di luce ambientale o sensori ambientali in grado di misurare la pressione atmosferica, la temperatura e l'umidità) e le aspettative degli incaricati a una "*interazione continua*".
L'uso misto di dispositivi mobili sia per scopi privati che professionali può portare un ulteriore livello di complessità. I dati personali trattati nell'ambito della vita professionale potrebbero essere trattati senza autorizzazione e la loro riservatezza, integrità e disponibilità compromessa durante l'utilizzo del dispositivo per scopi privati e viceversa, anche all'insaputa dell'utente.
I rischi più rilevanti per i dati personali sono:

- perdita accidentale di dati personali;
- alterazione o distruzione dei dati personali a causa di un accesso illegale da parte degli amministratori di dispositivi mobili, compreso lo spegnimento remoto e l'alterazione / cancellazione remota dei dati personali (foto, video, contatti locali, copie locali di e-mail, documenti, eccetera.);
- fuga di dati personali dovuta all'accesso non autorizzato a tali dati che potrebbe anche causare danni alla reputazione o finanziari al Titolare;
- localizzazione geografica illecita dell'incaricato da parte di potenziali aggressori tramite servizi di localizzazione;
- furto di identità attraverso la compromissione di credenziali (nomi utente, password, certificati) memorizzate su dispositivi mobili.

Le minacce più rilevanti che potrebbero portare ai rischi precedenti sono:

- applicazioni mobili e/o dispositivi mobili che raccolgono ed elaborano illecitamente dati personali;
- personalizzazione da parte di produttori di dispositivi, operatori e sviluppatori di sistemi operativi che portano a configurazioni e funzionalità bloccate;
- sfruttamento intenzionale da parte di hacker (esterni o interni) delle vulnerabilità dei dispositivi mobili per prendere di mira i dati personali (direttamente o come effetto collaterale del targeting dei dati aziendali);
- perdita o furto accidentale del dispositivo mobile;
- manomettere fisicamente il dispositivo per accedere alle informazioni in esso contenute o per installare malware;
- abuso;
- errore umano.

## 7.1. Violazione dei dati memorizzati

Se non sono in atto misure adeguate per proteggere i dati archiviati sui dispositivi mobili da accessi non autorizzati o inappropriati, il Titolare potrebbe essere esposto a potenziali danni finanziari, reputazionali o anche fisici, pertanto l'uso del BYOD in assenza di misure adeguate per proteggere i dati non è consentito.

## 7.2. Trattamento di "dati personali di terzi"

Alcuni dei dati personali trattati tramite dispositivi mobili si riferiscono a soggetti che non sono membri del personale del Titolare: dati personali di terzi.
Se consideriamo che i dispositivi mobili sono soggetti a maggiori rischi di perdita o furto e che le misure di sicurezza che possono essere implementate su un dispositivo mobile sono limitate, è evidente che i rischi per la protezione dei dati sono notevolmente più alti in questo scenario, pertanto i dati personali di terzi sono considerati "*critici*" alla pari dei dati personali dei lavoratori del Titolare.

## 7.3. Intercettazione delle comunicazioni

L'intercettazione delle comunicazioni può essere definita come l'osservazione o il monitoraggio delle comunicazioni o delle attività di un individuo. Il monitoraggio delle attività di qualcuno avviene tipicamente in tre modi:

1. ascoltando a sua insaputa la comunicazione;
2. ispezionando i dati raccolti dalle attività di comunicazione (metadati);
3. ottenendo l'accesso al dispositivo mobile stesso.

Pertanto, sui dispositivi BYOD il Titolare non può intercettare comunicazioni senza aver prima raccolto il consenso esplicito e circostanziato da parte dell'incaricato.

## 7.4. Rischi specifici BYOD

La possibilità per gli incaricati di utilizzare ("*portare*") i propri dispositivi mobili per accedere alle informazioni istituzionali può portare alcuni vantaggi sia al Titolare che agli incaricati. Tuttavia, questo comporta anche rischi aggiuntivi. Il grado di controllo che il Titolare e i dipartimenti IT possono esercitare, anche per quanto riguarda la configurazione dei dispositivi, è ridotto nello scenario BYOD rispetto a uno scenario in cui i dispositivi e le app sono preselezionati, approvati e gestiti dal Titolare.
Se il dispositivo mobile si connette alla rete del Titolare presenta un rischio aggiuntivo (anche a causa dell'impossibilità di gestire la sicurezza del dispositivo mobile). Le applicazioni non autorizzate e il malware possono utilizzare il dispositivo personale per intromettersi in una rete protetta.
Come notato, BYOD porta alla sfocatura dell'uso personale e professionale. Il Titolare rischia di avere accesso ai dati personali e privati degli incaricati (es. accedendo ai dati personali sincronizzati con l'infrastruttura istituzionale), e gli incaricati rischiano di esporre le informazioni istituzionali attraverso l'uso di servizi personali come il cloud storage o il backup (facilmente attivabili dagli incaricati stessi), o tramite applicazioni installate per usi personali che potrebbero successivamente offrire "*gateway*" per l'accesso illecito alle informazioni detenute dal Titolare.
L'ampia offerta sul mercato di diversi modelli di dispositivi mobili che utilizzano diversi sistemi operativi rende difficile se non impossibile per i dipartimenti IT del Titolare fornire supporto nella scelta e nella gestione di tutti questi dispositivi. Inoltre, il reparto IT difficilmente ha controllo sugli aggiornamenti e le configurazioni di sicurezza che possono essere applicati dall'utente o dal fornitore del dispositivo mobile. Tuttavia, la complessità e la difficoltà, sia da un punto di vista giuridico che tecnico, degli aspetti di protezione dei dati del trattamento dei dati da parte del Titolare da parte di un'infrastruttura informatica che utilizza dispositivi mobili forniti agli incaricati, non sono utilizzati dal Titolare come giustificazione in caso di mancato rispetto del regolamento. In definitiva, se il trattamento dei dati comporta il trattamento di dati e informazioni particolarmente sensibili, il Titolare non consente l'uso di dispositivi mobili (di proprietà istituzionale e/o BYOD) per la raccolta, l'archiviazione e la trasmissione di questi dati personali.

## 8. Norme di rinvio.

Per quanto non espressamente disciplinato nel presente si applicano le disposizioni di cui al codice in materia di protezione di dati personali e, per la parte ad essi attinenti, del Regolamento per la disciplina delle modalità del diritto di accesso ai documenti amministrativi, e dei singoli Regolamenti e disposizioni relativi al funzionamento del Titolare.

## 9. Entrata in vigore.

Il presente entrerà in vigore il giorno successivo a quello di esecutività della relativa deliberazione di approvazione e resterà in vigore fino ad atto contrario.

# Sommario

1. Premessa ..... 2
1.1. Vantaggi del BYOD ..... 2
1.2. Svantaggi del BYOD ..... 2
2. Introduzione ..... 2
2.1. Background tecnico ..... 3
3. Ambito, metodologia e struttura ..... 4
3.1. Scopo ..... 4
3.2. Metodologia ..... 4
3.3. Struttura ..... 5
4. Istruzioni operative ..... 5
4.1. R1: Titolare e DPO ..... 6
4.2. R2: Analisi costi / benefici ..... 6
4.3. R3: Uso accettabile della policy ..... 6
4.4. R4: Valutazione d'impatto sulla protezione dei dati (DPIA) ..... 6
4.5. R5: Risk Management ..... 6
4.6. R6: Data Breach ..... 6
4.7. R7: BYOD ..... 6
4.8. R8: Rettifica, blocco o cancellazione ..... 7
4.9. R9: Notifica al Garante ..... 7
5. Misure di sicurezza per proteggere i dati personali trattati nei dispositivi mobili ..... 7
5.1. Misure organizzative ..... 7
5.1.1. Gestione del ciclo di vita del dispositivo mobile ..... 7
5.1.2. Politica di sicurezza delle informazioni ..... 8
5.1.3. Formazione e Sensibilizzazione ..... 8
5.1.4. Misure organizzative per BYOD ..... 8
5.1.5. Violazioni della sicurezza / incidenti di sicurezza ..... 8
5.2. Misure tecniche ..... 8
5.2.1. Gestione dei dispositivi mobili (MDM) ..... 9
5.2.2. Altre misure tecniche ..... 10
6. Problemi di protezione dei dati relativi al trattamento dei dati personali tramite dispositivi mobili ..... 10
6.1. V.1 – Titolare del trattamento dati ..... 10
6.2. V.2 - Obbligo di sicurezza ai sensi del regolamento ..... 12
6.3. V.3 - Valutazione dell'impatto sulla protezione dei dati (DPIA) ..... 13
6.3.1. Descrizione sistematica del trattamento ..... 13
6.3.1.1. Natura, ambito di applicazione, contesto e finalità del trattamento ..... 13
6.3.1.1.1. Misure, garanzie e meccanismi previsti per attenuare il rischio MEDIO ..... 13
6.3.2. Destinatari e periodo di conservazione ..... 15
6.3.3. Risorse ..... 15
6.3.4. Necessità e proporzionalità dei trattamenti ..... 15
6.3.4.1. Misure per garantire il rispetto al GDPR ..... 15
6.3.4.1.1. Proporzionalità e necessità ..... 15
6.3.4.1.2. Misure che contribuiscono ai diritti degli interessati ..... 17
6.3.4.1.3. Gestione dei rischi per i diritti e le libertà degli interessati ..... 25
6.4. V.4 - Comunicazione delle violazioni dei dati ..... 26
6.5. V.5 - Archiviazione secondaria dei dati personali tramite dispositivi mobili ..... 26
7. Rischi per i dati personali trattati da dispositivi mobili ..... 26
7.1. Violazione dei dati memorizzati ..... 28
7.2. Trattamento di "dati personali di terzi" ..... 28
7.3. Intercettazione delle comunicazioni ..... 28
7.4. Rischi specifici BYOD ..... 28
8. Norme di rinvio. ..... 29
9. Entrata in vigore. ..... 29