2023

Regolamento per la gestione e la protezione dei dati personali

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

Titolare del trattamento: Fondazione MAXXI – MUSEO DELLE ARTI DEL XXI SECOLO
t: 063201954
e: privacy@fondazionemaxxi.it

Sede interessata: Fondazione MAXXI, via G. Reni 4/A – 00196 Roma; MAXXI L'Aquila, Piazza Santa Maria Paganica, 5 – 67100 L'Aquila

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale
delle arti del XXI secolo

I PARTE

1. **Definizioni**
2. **Principi e novità**
3. **Processo di adeguamento al GDPR della Fondazione MAXXI**
4. **Compiti del titolare del trattamento**
5. **Compiti del responsabile del trattamento**
6. **Compiti degli addetti autorizzati al trattamento**
7. **Compiti del responsabile della protezione dei dati personali**
8. **Gestione del rischio**
9. **Valutazione di impatto (PIA)**
10. **Diritti degli interessati**
11. **Raccolta del consenso e informative**
12. **Sanzioni**

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

1. DEFINIZIONI

Il **dato personale** è qualsiasi informazione riguardante una persona fisica identificata o identificabile (l'interessato). È identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, i dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Come in tutte le definizioni riferite ai dati, il Regolamento (UE) n. 2016/679 usa l'espressione *qualunque informazione* anche per indicare un numero di telefono o il codice fiscale, anche se non direttamente collegati al nome dell'interessato. Ciascuno di essi sono dati personali.

I dati personali si distinguono in dati comuni, dati particolari e dati giudiziari penali.

Ai dati comuni appartengono tutte quelle informazioni come nome, cognome, partita iva, codice fiscale, indirizzo, numero di telefono, numero di carta di identità, che consentono di individuare una persona fisica. Tali dati, pur non sussistendo particolari esigenze di protezione, devono comunque sottostare ai principi generali che regolano il trattamento dei dati, in particolare, i principi di minimizzazione e di esattezza, ragione per cui essi devono essere raccolti soltanto quando risultano indispensabili e per finalità per individuate.

I dati particolari sono solo i dati specificamente indicati nel Regolamento, indipendentemente dal carattere di riservatezza o di particolare rilevanza che ciascun individuo può attribuire al dato (ad esempio un codice identificativo della carta di credito o il reddito). Si tratta delle informazioni che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Ad esempio, il livello di stipendio di un lavoratore è di per sé un dato comune; il cedolino dello stipendio può, però, recare informazioni di tipo particolare (la ritenuta sindacale o le trattenute per malattia), per cui deve rimanere riservato.

Infine, i dati giudiziari penali sono quei dati personali relativi a condanne penali e reati o connessi a misure di sicurezza. Sono esclusi dal novero, i dati giudiziari di natura civilistica.

Il **trattamento** è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Va precisato che non si considera comunicazione lo scambio di informazioni tra strutture interne allo stesso Ente o tra queste e soggetti esterni individuati come responsabili del trattamento, nell'ambito dell'attività di outsourcing o in base ad altro atto o contratto. La comunicazione per diffusione avviene, ad esempio, mediante l'inserimento dei dati personali su un sito internet, su un comunicato stampa, su un giornale, su un documento lasciato incustodito.

L'**archivio** è qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Il **titolare del trattamento** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Il **responsabile del trattamento** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Il **destinatario** è la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Il **terzo** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Il **consenso dell'interessato** è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

La **violazione dei dati personali** è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

L'**Autorità di controllo** è l'autorità pubblica indipendente istituita da uno Stato Membro, incaricata della sorveglianza dell'attuazione del Regolamento (UE) 2016/679.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

2. PRINCIPI E NOVITA'

La protezione dei dati delle persone fisiche è un diritto fondamentale riconosciuto dalla Carta dei Diritti Fondamentali dell'Unione Europea e dal Trattato sul funzionamento dell'Unione Europea.

Con il Regolamento (UE) n. 2016/679 la Commissione Europea ha inteso rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini europei.

Il Regolamento (UE) – altrimenti detto GDPR – fa parte di un insieme di norme che definisce il nuovo quadro in materia di tutela dei dati personali per tutti gli Stati Membri dell'UE e comprende anche la Direttiva in materia di trattamento dei dati personali nei settori della prevenzione, contrasto e repressione dei crimini.

Dal 25 maggio 2018, in tutti i Paesi dell'Unione Europea, il GDPR ha sostituito la direttiva sulla protezione dei dati personali (Direttiva 95/46/EC) e ha trovato applicazione immediata e diretta.

Le disposizioni contenute nel GDPR incidono sulla organizzazione interna degli Enti, modificando gli assetti strutturali e le responsabilità.

In particolare, è introdotta la responsabilità diretta dei titolari del trattamento in merito al compito di assicurare, ed essere in grado di dimostrare – *accountability* – il rispetto dei principi applicabili al trattamento dei dati personali; è definita la nuova categoria dei dati personali; viene istituita la figura del Responsabile della Protezione dei Dati personali (DPO) incaricato di assicurare una gestione corretta dei dati personali; viene introdotto il registro delle attività del trattamento ove sono descritti i trattamenti effettuati e le procedure di sicurezza adottate dall'ente; viene richieste di effettuare una valutazione di impatto sulla protezione dei dati, prima di procedere al trattamento.

Tutto ciò avviene perché, diversamente dal passato, il nuovo assetto non è più basato su un disciplinare tecnico delle misure minime di sicurezza, essendo posto a carico del titolare la responsabilità di definire, all'esito di una attenta analisi dei rischi, le misure di sicurezza idonee a garantire la protezione dei dati personali trattati. Costituisce una novità, rispetto al passato, la previsione che, per mantenere la sicurezza e prevenire trattamenti commessi in violazione del GDPR, il titolare del trattamento debba valutare i rischi inerenti al trattamento e attuare misure adeguate per limitare tali rischi. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché dell'oggetto, del contesto e delle finalità del trattamento, del rischio di varia probabilità e gravità per le persone fisiche, il titolare deve mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. L'elenco delle misure indicate nel GDPR è meramente esemplificativo e non esaustivo.

Il GDPR afferma i principi che dovranno trovare applicazione al trattamento dei dati personali: essi sono la *liceità, la correttezza e la trasparenza del trattamento, la minimizzazione, la limitazione della conservazione, la finalità del trattamento*, la *responsabilizzazione*.

Costituisce diretta e concreta applicazione di questi principi la previsione di specifici d*iritti dell'interessato*: il diritto di accesso alle informazioni, il diritto alla rettifica e alla cancellazione delle informazioni, il diritto di limitazione del trattamento, il diritto alla portabilità dei dati, il diritto di opposizione al trattamento.

Il GDPR conferma, poi, la regola per cui, ai fini della sua liceità, il trattamento dei dati deve trovare fondamento in una idonea base giuridica che, oltre al consenso, è individuata nell'esecuzione di un

contratto di cui l'interessato è parte o di misure precontrattuali adottate su richiesta dello stesso; nell'adempimento di un obbligo di legge al quale è soggetto il titolare del trattamento; nella salvaguardia di interessi vitali dell'interessato o di un'altra persona fisica; nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; nel perseguimento di un legittimo interesse del titolare.

Ulteriore novità rispetto al passato, è la previsione di Registri delle attività di trattamento, aventi contenuto specifico, che servono ad individuare le categorie di dati trattati e le categorie di persone interessate, le finalità del trattamento, i dati di contatto del titolare, del contitolare, del rappresentante e del responsabile della protezione dei dati. Tali registri sono detenuti sia dal titolare del trattamento che dal responsabile del trattamento.

Specifica attenzione viene infine data agli obblighi di comunicazione delle violazioni dei dati personali (c.d. data breach), sia nei confronti dell'Autorità di controllo sia, se del caso, alle persone interessate.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

3. IL PROCESSO DI ADEGUAMENTO AL GDPR DELLA FONDAZIONE MAXXI

La Fondazione MAXXI ha adottato il presente Regolamento per garantire che tutti i trattamenti effettuati si svolgano nel rispetto dei diritti e delle libertà fondamentali dell'interessato e il rispetto delle norme sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati.

A tal fine, la Fondazione ha eseguito la mappatura dei trattamenti eseguiti, individuando le aree interessate, le finalità e la base giuridica dei trattamenti, i soggetti autorizzati al trattamento, le misure di sicurezza adottate, partendo dall'analisi della documentazione esistente (Atto costitutivo della Fondazione, Statuto della Fondazione, Organigramma, provvedimenti in materia di protezione dei dati personali ai sensi del D.Lgs. n. 196/2003, altri provvedimenti specifici) ed intervistando i responsabili delle Aree/Funzioni. All'esito dell'analisi sono stati ricostruiti i seguenti trattamenti.

Il risultato è stato la redazione del Registro dei trattamenti nel quale sono indicati i dati identificativi e di contatto del titolare del trattamento, le finalità dei trattamenti, le categorie delle persone interessate, le categorie dei dati trattati, i termini di conservazione delle categorie di dati, la descrizione generale delle misure di sicurezza tecniche e organizzative adottate, le persone autorizzate al trattamento.

All'esito della mappatura dei trattamenti effettuati dalla Fondazione, sono stati individuati i ruoli e le responsabilità per la sicurezza delle informazioni, in relazione alla struttura della Governance della Fondazione.

Successivamente all'individuazione dei soggetti coinvolti nei trattamenti dei dati personali si è proceduto a redigere le lettere di incarico per i responsabili del trattamento – soggetti esterni alla struttura che sulla base di contratti, appalti, convenzioni, trattano dati personali di cui la Fondazione è titolare – e per gli addetti autorizzati al trattamento – soggetti che, alle dipendenze del Titolare o comunque che agiscono sotto la sua autorità –, con le contestuali istruzioni. Con riferimento ai primi, la Fondazione ha individuato soggetti che assicurano il rispetto della normativa per il trattamento dei dati loro affidati, impegnando gli stessi ad adottare tutte le misure di sicurezza, tecniche ed organizzative, adeguate per la protezione dei dati.

Con riferimento agli addetti autorizzati al trattamento, la Fondazione ha incaricato chiunque utilizza dati personali di qualsiasi tipo. L'individuazione è stata effettuata descrivendo l'ambito di trattamento consentito, precisando quali dati l'incaricato può trattare relativamente alle funzioni del suo ufficio e in che modo vanno trattato.

L'individuazione degli incaricati non è atto recettizio, pertanto, non è firmato per accettazione bensì per ricevuta, al fine di dimostrare che l'addetto ha ricevuto l'atto di incarico e le istruzioni.

Al fine di ottemperare al dovere di adottare misure tecniche ed organizzative adeguate per la protezione delle informazioni trattate, la Fondazione ha effettuato una ampia valutazione dei rischi per i diritti e le libertà degli interessati, connessi ai vari trattamenti effettuati, individuando, tra le altre cose, le azioni da adottare per ridurre il pericolo di perdita, distruzione o sottrazione delle informazioni. Si è poi proceduto ad una specifica valutazione di impatto (PIA) per quel che riguarda il trattamento di dati relativi allo stato di salute di taluni dipendenti, assunti in base alla normativa sulle categorie protette di lavoratori, in osservanza a quanto statuito dall'Autorità Garante per la protezione dei dati personali.

Sono stati altresì individuati generali protocolli comportamentali, oltre alle istruzioni specificamente previste per gli addetti al trattamento.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale delle arti del XXI secolo

4. COMPITI DEL TITOLARE DEL TRATTAMENTO

La Fondazione MAXXI, nella qualità di titolare del trattamento dei dati personali, è tenuta a:

- Rispettare i principi e le norme nazionali ed europee vigenti in materia di trattamento dei dati personali.
- Individuare, nominare ed istruire chiunque agisce sotto la sua autorità e ha accesso ai dati personali.
- Individuare, nominare e istruire i responsabili del trattamento che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del Regolamento (UE) n. 2016/679 e delle norme vigenti in materia. La nomina viene effettuata mediante atto giuridico scritto, indicando i compiti assegnati, a norma del diritto nazionale ed europeo.
- Eventualmente autorizzare il responsabile del trattamento a ricorrere ad altro responsabile mediante atto scritto e specifico.
- Ove applicabile, designare per iscritto un rappresentante nel territorio dell'Unione Europea incaricato di affrontare tutte le questioni riguardanti il trattamento dei dati neri rapporti con le Autorità di controllo e gli interessati.
- Determinare, eventualmente, insieme ad altri titolari del trattamento, mediante accordo interno, le finalità e i mezzi del trattamento, mettendo a disposizione degli interessati il contenuto essenziale dell'accordo.
- Individuare i trattamenti di dati personali in corso.
- Assumere le decisioni strategiche sulle modalità e le ragioni della raccolta e del trattamento dei dati, sull'organizzazione del trattamento e sulle risorse da utilizzare, anche per garantire la sicurezza delle informazioni.
- Tenere il registro delle attività di trattamento svolte sotto la propria responsabilità.
- Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mettere in atto misure tecniche ed organizzative adeguate per garantire e dimostrare che il trattamento è conforme al Regolamento (UE) n. 2016/679 e alle norme vigenti in materia.
- Riesaminare e aggiornare, quando necessario, le misure tecniche ed organizzative.
- Adottare misure appropriate per fornire agli interessati tutte le informazioni e le comunicazioni previste dalle norme di legge, relative al trattamento dei dati personali.
- Cooperare con l'Autorità Garante nell'esecuzione dei suoi compiti.
- Notificare la violazione dei dati personali all'Autorità Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza, nei casi e alle condizioni previste dalle norme di legge.
- Comunicare la violazione dei dati personali agli interessati, nei casi e alle condizioni previste dalle norme di legge.
- Eventualmente effettuare una valutazione di impatto dei trattamenti in corso sulla protezione dei dati personali, alle condizioni previste dalle norme di legge, consultando, se del caso, l'Autorità Garante.
- Nominare il Responsabile per la Protezione dei Dati personali.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

5. COMPITI DEL RESPONSABILE DEL TRATTAMENTO

I trattamenti effettuati da parte del Responsabile del trattamento sono disciplinati da un contratto o altro atto giuridico che individua la durata, la natura, la finalità del trattamento, il tipo di dati personali e le categorie degli interessati, le responsabilità affidate al responsabile, gli obblighi e i diritti del titolare.

Il responsabile del trattamento deve:

- Trattare i dati personali secondo le istruzioni impartite dalla Fondazione MAXXI e, in caso di trattamenti particolarmente complessi, può nominare a sua volta, previa autorizzazione scritta e specifica della Fondazione, un sub responsabile. In caso di nomina di altro responsabile, il Responsabile deve fornire alla Fondazione i dettagli completi sul trattamento dei dati da parte di altri responsabili; effettuare una *due diligence* su ciascun responsabile aggiunto per garantire che possa fornire il livello di protezione dei dati personali trattati per conto della Fondazione, incluse sufficienti garanzie per mettere in atto misure tecniche ed organizzative appropriate; su richiesta, fornire alla Fondazione una copia degli accordi con altri responsabili per la sua revisione; incorporare clausole di riservatezza per la protezione delle informazioni; rimanere responsabile nei confronti della Fondazione per qualsiasi mancanza da parte di ciascun altro responsabile nell'adempiere agli obblighi sulla protezione dei dati personali.
- Assistere la Fondazione nell'osservanza delle misure tecniche ed organizzative adeguate e nel rispetto dei doveri in tema di sicurezza, valutazione di impatto sulla protezione dati e consultazione preventiva di cui al GDPR, e dare seguito alle istanze di accesso dell'interessato.
- Permettere alla Fondazione, o ad altro soggetto da lei incaricato, di accedere, ai fini della verifica della conformità alla normativa in materia, a tutte le informazioni di cui dispone, anche mediante *audit*.
- Raggiungere un sufficiente grado di conoscenza della normativa sulla protezione dei dati personali in modo da trattare le informazioni secondo legge.
- Adottare tutte le misure di sicurezza richieste dalla legge.
- Cancellare o restituire, a scelta della Fondazione, tutti i dati personali dopo che è terminata la prestazione del servizio relativa al trattamento, e cancellare le copie esistenti.
- Interagire con l'Autorità Garante in caso di richieste di informazioni, di controlli o di accessi.
- Informare la Fondazione se riceve una richiesta dall'Autorità Garante o da altra Autorità.
- Informare la Fondazione se riceve una richiesta da un interessato.
- Soddisfare le richieste degli interessati, in base all'esercizio dei loro diritti.
- Il Responsabile dovrà cooperare con la Fondazione per consentire: la fornitura di tutti i dati richiesti dalla Fondazione, entro un tempo ragionevole indicato dal titolare, comprese le informazioni e le copie del reclamo, della comunicazione o della richiesta e qualsiasi altro dato personale relativo all'interessato; fornire assistenza alla Fondazione per consentirgli di soddisfare la relative richiesta entro i termini prescritti dalla normativa di settore; implementare eventuali misure tecniche e organizzative aggiuntive che possano essere ragionevolmente richieste dalla Fondazione per consentire di rispondere in modo efficace a reclami, comunicazioni o richieste pertinenti.
- Trattare i dati per conto della Fondazione ai soli fini dell'esecuzione dell'incarico ricevuto. In tal caso il Responsabile non deve trattare, trasferire o divulgare o consentire la divulgazione a terzi se non in conformità alle istruzioni documentate della Fondazione, a meno che il trattamento non sia richiesto dall'UE e/o dalle leggi dello Stato Membro a cui è soggetto il Responsabile e/o una qualsiasi legislazione anche sovranazionale a cui è soggetto il Responsabile. Il Responsabile del trattamento dovrà, nella misura consentita da tali leggi, informare la Fondazione di tali requisiti

legali prima di trattare i dati personali e attenersi alle istruzioni della Fondazione per ridurre al minimo, per quanto possibile, l'ambito di divulgazione.

- Detenere e aggiornare regolarmente un registro di tutte le categorie di attività relative al trattamento svolte per conto della Fondazione, contenente il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie adeguate; ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.
- Individuare gli incaricati al trattamento che garantiscano affidabilità e correttezza nell'accesso ai dati personali degli interessati. In tal caso, il Responsabile garantisce che tutti gli addetti siano informati della natura confidenziale dei dati trattati per conto della Fondazione e siano a conoscenza degli obblighi del Responsabile; siano in possesso di adeguata formazione in relazione alla materia della protezione dei dati personali; siano soggetti a impegni di riservatezza o obblighi professionali di riservatezza; siano soggetti all'autenticazione dell'utente e alle procedure di accesso quando accedono ai dati personali trattati per conto della Fondazione in conformità all'accordo.
- Informare prontamente la Fondazione di ogni questione rilevante ai fini del trattamento e della protezione dei dati personali.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

6. COMPITI DEGLI ADDETTI AUTORIZZATI AL TRATTAMENTO

La Fondazione individua e nomina quali addetti, autorizzati al trattamento, tutti i dipendenti, collaboratori, consulenti, e altri soggetti che intervengono, in relazione all'esercizio delle rispettive mansioni e competenze, nell'esecuzione dei trattamenti ed operano sotto l'autorità della Fondazione.

Sono addetti, autorizzati al trattamento dei dati, tutti i soggetti di cui sopra, assegnati alle aree della Fondazione secondo l'ultimo organigramma adottato.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale delle arti del XXI secolo

7. COMPITI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

Ricorrendo le ipotesi di cui all'art. 37 n. 1 lettere a), b), c) del Regolamento (UE) n. 2016/679 la Fondazione designa un Responsabile della Protezione dei dati con comprovate conoscenze in materia di privacy, i cui contatti sono comunicati all'Autorità di controllo.

Il Responsabile della Protezione dei dati può essere un dipendente della Fondazione o un soggetto esterno nominato in virtù di un contratto di servizi.

il Responsabile della Protezione dei Dati:

- informa e fornisce consulenza alla Fondazione o al Responsabile del trattamento.
- vigila sull'osservanza della normativa in materia di protezione dei dati personali, compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale che partecipa ai trattamenti.
- Fornisce pareri, se richiesti, al titolare del trattamento.
- Coopera con l'autorità di controllo.
- Funge da punto di contatto per l'Autorità di controllo per le questioni legate al trattamento ed effettua, se del caso, consultazioni relativamente a qualunque altra questione.
- Viene coinvolto dalla Fondazione o dal Responsabile in tutte le questioni riguardanti la protezione dei dati personali.
- Assolve i compiti prescritti con le risorse necessarie messe a disposizione dalla Fondazione.
- Mantiene la propria conoscenza specialistica con il sostegno delle risorse messe a disposizione dalla Fondazione
- Non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti
- Non può essere rimosso o penalizzato per l'adempimento dei propri compiti.
- Riferisce direttamente al vertice gerarchico della Fondazione
- Può essere contattato dagli interessati per tutte le questioni relative al trattamento dei loro dati personali o all'esercizio dei loro diritti.
- È tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti.
- Può svolgere altre funzioni o compiti, purchè non in conflitto di interessi.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale
delle arti del XXI secolo

8. GESTIONE DEL RISCHIO

La Fondazione MAXXI definisce il processo di valutazione dei rischi e un processo di valutazione di impatto sulla protezione dei dati personali oggetto di trattamento che permette di:

- identificare il rischio per i diritti e le libertà delle persone fisiche e, nel caso in cui ricorre una violazione dei dati personali, anche per la Fondazione.
- valutare le misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio
- fornire le necessarie garanzie al fine di soddisfare i requisiti normativi di riferimento

In particolare, il processo di valutazione dei rischi permette di stabilire e mantenere i criteri di accettazione del rischio relativo alla protezione dei dati personali e quelli per l'esecuzione della valutazione del rischio; identifica, altresì, i rischi associati al non rispetto delle norme di legge, all'impatto sui diritti e le libertà delle persone e all'impatto sull'organizzazione; analizza la verosimiglianza del concretizzarsi dei rischi indentificati e le potenziali conseguenze che risulterebbero se i rischi identificati dovessero concretizzarsi; determina i livelli di rischio; pondera i rischi relativi alla protezione dei dati personali.

Il processo di valutazione, contenuto in un documento denominato Analisi dei Rischi, viene revisionato con periodicità semestrale o annuale, o comunque quando intervengono cambiamenti significativi nelle modalità o negli strumenti utilizzati per svolgere l'attività di trattamento.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale
delle arti del XXI secolo

9. VALUTAZIONE DI IMPATTO (PIA)

La Fondazione Maxxi intende garantire il rispetto dei requisiti di compliance in materia di protezione dei dati personali.

Pertanto, prima di procedere a trattamenti particolari, la Fondazione ha effettuato una valutazione dell'impatto del trattamento nei casi in cui esso presenta un rischio elevato per i diritti e le libertà degli interessati.

Si è proceduto ad individuare:

- le ragioni per cui il Titolare ritiene necessaria la valutazione
- i flussi informativi – ovvero le categorie di dati oggetto di trattamento, gli utilizzatori, le sorgenti e i destinatari finali del dato –
- i rischi, mediante analisi, in termini di probabilità e gravità, delle minacce che potrebbero concretizzarsi procurando in danno all'interessato
- le soluzioni al fine di ridurre la probabilità di verifica dell'evento.

Sulla base del Provvedimento n. 467 dell'11 ottobre 2018 dell'Autorità Garante per la Protezione dei Dati Personali, la Fondazione ha individuato le seguenti categorie di trattamento da sottoporre a valutazione di impatto:

- trattamento non occasionale di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

10. DIRITTI DEGLI INTERESSATI

La Fondazione riconosce all'interessato l'esercizio dei seguenti diritti:

- DIRITTO DI ACCESSO. L'interessato ha diritto di sapere che è in corso un trattamento di dati personali che lo riguardano e di ottenerne l'accesso, insieme alle seguenti informazioni: le finalità del trattamento, le categorie dei dati trattati, gli eventuali destinatari degli stessi, il periodo di conservazione, gli altri diritti azionabili – tra cui quello di proporre reclamo all'autorità di controllo, l'origine dei propri dati nel caso questi siano stati raccolti pressi terzi, l'esistenza di processi decisionali automatizzati, ad esempio la profilazione.
- DIRITTO DI RETTIFICA. La Fondazione è tenuta a rettificare, senza ingiustificato ritardo, i dati personali inesatti che riguardano l'interessato o ad integrare quelli incompleti.
- DIRITTO ALLA CANCELLAZIONE. L'interessato ha il diritto di ottenere da parte della Fondazione la cancellazione dei dati che lo riguardano, qualora ricorrano i motivi di cui all'art. 17 del Regolamento (UE) n. 2016/679.
- DIRITTO DI LIMITAZIONE DEL TRATTAMENTO. Nelle ipotesi di cui all'art. 18 del Regolamento (UE) n. 2016/679, l'interessato ha diritto di ottenere dal Titolare la limitazione del trattamento dei dati che lo riguardano.
- DIRITTO ALLA PORTABILITA' DEI DATI. Salvo che non ricorrano le ipotesi previste dalla legge, 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 al Titolare del trattamento e di trasmetterli, senza impedimenti, ad un altro Titolare.
- DIRITTO DI OPPOSIZIONE. l'interessato ha il diritto di opporsi in qualunque momento al trattamento dei dati personali, salvo che il trattamento non sia giustificato da motivi legittimi prevalenti rispetto agli interessi, diritti e libertà dell'interessato.
- SICUREZZA DEL TRATTAMENTO. La Fondazione garantisce un livello di sicurezza adeguato al rischio per i diritti e le libertà degli interessati, adottando misure tecnico-organizzative, fra le quali:
- la pseudonimizzazione e la cifratura dei dati personali.
- la capacità di assicurare permanentemente la riservatezza, l'integrità, la disponibilità, nonchè la resilienza dei sistemi e dei servizi di trattamento.
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali e, in generale, la manutenzione dei sistemi informatici.
- una procedura per testare regolarmente l'efficacia delle misure adottate per prevenire e/o fronteggiare i potenziali rischi del trattamento.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale delle arti del XXI secolo

11. RACCOLTA DEL CONSENSO E INFORMATIVE

La Fondazione acquisisce il consenso dell'interessato al momento della raccolta o prima della raccolta dei dati personali, per qualsiasi tipo di attività di trattamento, quando è necessario ai sensi del Regolamento (UE) n. 2016/679, informando adeguatamente gli interessati sul tipo di dati personali raccolti, sulle finalità del trattamento, sui metodi di trattamento, sui diritti degli interessati, sul periodo di conservazione, sui potenziali trasferimenti internazionali dei dati, se i dati saranno condivisi con terzi e sulle misure di sicurezza adottate per proteggere i dati personali.

Contestualmente o preventivamente alla raccolta delle informazioni viene fornita all'interessato l'informativa sul trattamento dei dati personali: essa può essere considerata un vero e proprio biglietto di visita dell'Ente e, pertanto, deve essere chiara e completa, mantenuta aggiornata rispetto ai cambiamenti significativi delle finalità e modalità di trattamento.

L'informativa contiene:

- l'identità e i dati di contatto del titolare del trattamento
- i dati di contatto del responsabile della protezione dei dati personali
- le finalità e la base giuridica del trattamento
- i legittimi interessi perseguiti dal titolare o da terzi
- gli eventuali destinatari o le categorie di destinatari dei dati personali
- l'intenzione del titolare del trattamento di trasferire dati all'estero
- il periodo di conservazione dei dati
- l'elencazione dei diritti dell'interessato
- l'obbligo legale o contrattuale di comunicare i dati nei casi previsti
- l'esistenza di un processo decisionale automatizzato

Nel caso in cui vengono raccolti dati comuni e particolari, la Fondazione si assicura che l'informativa sul trattamento dei dati personali, ai sensi degli artt. 13 e 14 del Regolamento (UE) n. 2016/679, sia stata correttamente portata a conoscenza degli interessati. L'informativa viene conservata in duplice copia, in formato elettronico e cartaceo, presso l'area che per prima ha fornito il documento e presso l'area Amministrazione, finanza e bilancio. È pertanto opportuno inserire l'informativa in tutta la modulistica relative alle richieste dei dati da parte della Fondazione.

L'informativa è inserita anche nella home page del sito internet del Museo MAXXI.

Ogniqualvolta è richiesto il consenso dell'interessato, questo verrà conservato e custodito in modalità cartacea o elettronica, assicurando adeguate misure di sicurezza. L'interessato deve poter conoscere le modalità per poter prestare il consenso e ha diritto di revocarlo in qualsiasi momento. Quando vengono raccolti dati personali relativi a interessati di età inferiore ad anni 16, la Fondazione deve garantire che sia stato manifestato il consenso dell'esercente la responsabilità genitoriale, prima della raccolta.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

12. SANZIONI

Il mancato rispetto delle disposizioni in materia di protezione dei dati personali è sanzionato con l'applicazione delle sanzioni amministrative pecuniarie, con le modalità previste dall'art. 83 del Regolamento (UE) n. 2016/679.

Le sanzioni amministrative pecuniarie tengono conto della natura, della gravità e della durata della violazione, tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché del numero di interessati lesi dal danno e il livello di danno da essi subito; del carattere doloso o colposo della violazione; delle misure adottata dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; del grado di responsabilità del titolare del trattamento o del responsabile del trattamento, tenendo conto delle misure tecniche e organizzative da essi messe in atto; di eventuali precedenti violazioni; del grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; della categorie di dati personali interessate dalla violazione; della maniera in cui l'Autorità di controllo ha preso conoscenza della violazione; dell'adesione a codici di condotta approvati; di eventuali fattori aggravanti o attenuanti.

Sono soggette alla sanzione amministrativa pecuniaria sino a euro 10.000.000 o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, le violazioni relative a:

gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli artt. 8, 11, da 25 a 39, 42 e 43 del Regolamento (UE) n. 2016/679

Sono soggette alla sanzione amministrativa pecuniaria sino a euro 20.000.000 o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, le violazioni relative a:

i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli artt. 5, 6, 7 e 9 del Regolamento (UE) n. 2016/679

i diritti degli interessati a norma degli artt. da 11 a 22 del Regolamento (UE) n. 2016/679

i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli artt. da 44 a 49 del Regolamento (UE) n. 2016/679

qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo XI del Regolamento (UE) n. 2016/679

l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati all'Autorità di controllo ai sensi dell'art. 58, paragrafo 2, o il negato accesso in violazione dell'art. 58, paragrafo 1 del Regolamento (UE) n. 2016/679.

Resta in ogni caso ferma l'applicabilità delle sanzioni penali, conformemente a quanto previsto dalla legislazione nazionale in materia.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale
delle arti del XXI secolo

II PARTE

1. **Procedura per la raccolta dei dati**
2. **Procedura per la conservazione e lo smaltimento dei dati**
3. **Procedura per il ripristino dei dati**
4. **Procedura per la violazione dei dati**
5. **Procedura per la gestione delle richieste degli interessati**
6. **Non conformità e azioni correttive**
7. **Aggiornamento posizioni**
8. **Contratti e bandi**
9. **Videosorveglianza**
10. **Formazione**
11. **Linee guida per il trattamento di categorie particolari di dati in ambito lavorativo**
12. **Linee guida per la gestione dei sistemi informativi**

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

1. PROCEDURA PER LA RACCOLTA DEI DATI

La Fondazione MAXXI procede alla raccolta dei dati personali fornendo preventivamente l'informativa sul trattamento, espressa con un linguaggio semplice e chiaramente comprensibile, aggiornata rispetto ai mutamenti delle finalità o delle modalità di trattamento.

Le informative riportano la versione applicabile. Il titolare o il responsabile, per tutte le informative, devono conservare le versioni precedenti rispetto a quella applicabile in modo da tenere traccia di quanto è stato comunicato all'interessato nel tempo.

Nel caso in cui il trattamento non è fondato sul consenso, bensì su altre basi giuridiche (ad esempio, un contratto, un obbligo di legge, etc) va chiesta conferma della presa visione dell'informativa. L'informativa viene conservata in duplice copia, in formato elettronico e cartaceo, presso l'area che per prima ha fornito il documento e presso l'area Amministrazione, finanza e bilancio. È pertanto opportuno inserire l'informativa in tutta la modulistica relative alle richieste dei dati da parte della Fondazione.

L'informativa è inserita anche nella home page del sito internet del Museo MAXXI.

Nel caso in cui il trattamento è basato sul consenso, al termine della visualizzazione dell'informativa e prima di procedere al trattamento, deve essere richiesto un esplicito consenso, attraverso la compilazione di apposita modulistica.

Il consenso è:

- collegato ad una informativa tracciabile in modo univoco
- richiesto individualmente per ogni trattamento per cui il consenso costituisce la base legale (in particolare, il consenso deve essere richiesto in modo separato per diverse finalità come ad esempio quelle di profilazione/marketing)
- espresso liberamente e in modo consapevole, attraverso opzioni chiare.
- Raccolto con la registrazione di quanto è stato prestato e del momento in cui è stato accordato
- Richiesto nuovamente in caso di cambiamenti significativi alle finalità o alle modalità di trattamento presentate nell'informativa
- Revocabile con la stessa facilità con cui lo si può accordare

Il consenso è conservato insieme all'informativa presso l'area che per prima ha somministrato il documento.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

2. PROCEDURA PER LA CONSERVAZIONE E LO SMALTIMENTO DEI DATI

La Fondazione MAXXI prevede periodi standard di conservazione dei dati personali e fissa le modalità per procedere alla distruzione delle informazioni.

La procedura si applica:

- a tutti i dipendenti, consulenti, fornitori di servizi, collaboratori, amministratori, funzionari, dirigenti
- a tutte le aree della Fondazione
- a tutte le informazioni utilizzate dalla Fondazione (compresi documenti elettronici, cartacei, video e audio, email, dati generati da sistemi di controllo degli accessi fisici)

Il periodo di conservazione è di 1 anno dalla data di creazione del documento, fatto salvo quanto diversamente previsto dalla legge applicabile o da specifiche esigenze indicate nel Registro dei trattamenti. In ogni caso, il periodo di conservazione dei dati può essere prolungato quando:

- sono in corso indagini condotte dall'Autorità Giudiziaria
- occorre dimostrare la conformità della Fondazione agli obblighi di legge
- occorre esercitare un diritto o resistere, nel caso di procedimenti giudiziari

La Fondazione garantisce che le informazioni contenute sui supporti (elettronici o cartacei) utilizzati per l'archiviazione siano sempre disponibili durante il periodo di conservazione. La responsabilità per la conservazione degli archivi digitali ricade sul referente ICT dell'area manutenzione, tecnico e logistica della Fondazione.

La Fondazione pone a carico degli addetti incaricati del trattamento dei dati personali il dovere di riesaminare tutti le informazioni contenute sui supporti (elettronici o cartacei), al fine di decidere se distruggere o cancellare qualsiasi dato una volta che lo scopo per cui tali documenti sono stati realizzati si è esaurito.

Una volta assunta la decisione di smaltire i dati secondo il programma di conservazione, le informazioni dovranno essere cancellate e i supporti triturati o altrimenti distrutti. Le modalità di smaltimento dipendono dal valore, dal livello di riservatezza e dalla natura (comuni o particolari) dei dati personali.

I dipendenti devono svolgere i compiti necessari per lo smaltimento delle informazioni in modo appropriato.

Il referente ICT deve documentare e approvare pienamente il processo di distruzione.

Il Responsabile della protezione dei dati ha la responsabilità di garantire che ciascuna area della Fondazione rispetti questa policy.

La violazione effettiva o presunta di questa procedura deve essere immediatamente segnalata al responsabile dell'area che condurrà la relativa indagine e adotterà le azioni adeguate.

La mancata osservanza di queste procedure da parte dei dipendenti, dei collaboratori, di terzi in genere, ai quali è concesso l'accesso alle informazioni della Fondazione può comportare l'adozione di provvedimenti disciplinari.

Salvo che non sia in corso un procedimento o una indagine condotta dall'Autorità, possono essere regolarmente distrutti i seguenti documenti:

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

- comunicazioni di riunioni o di altri eventi quotidiani
- richieste di informazioni ordinarie
- trasmissioni di documenti quali lettere, copertine fax, email e simili che accompagnano i documenti ma non aggiungono valore
- duplicati di documenti, come copie inoltrate per conoscenza, bozze inalterate, estratti da database
- riviste di settore, cataloghi, volantini, newsletter provenienti da fornitori o da altri soggetti esterni

I documenti che contengono informazioni di massima sicurezza e riservatezza devono essere smaltiti come rifiuti riservati (distrutti con un tritacarte) e devono essere sottoposti a cancellazione elettronica sicura. Lo smaltimento dei documenti deve includere la prova della distruzione.

I documenti che contengono nomi, firme e indirizzi devono essere triturati e collocati in bidoni chiusi per essere raccolti da una ditta di smaltimento autorizzata; i documenti elettronici devono essere soggetti a cancellazione elettronica sicura.

I documenti che non contengono informazioni riservate o dati personali (inclusi cataloghi, pubblicità, volantini, newsletter) devono essere tagliati a strisce o eliminati elettronicamente.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale delle arti del XXI secolo

3. PROCEDURA PER IL RIPRISTINO DEI DATI

Il ripristino dei dati (back-up) viene effettuato dalla Fondazione MAXXI. Il back-up dei dati viene eseguito con schedulazione giornaliera tramite il software Veeam B&R. Viene eseguita una copia dei dati del file server tramite script tra sito di produzione e sito DR.

La Fondazione mantiene il controllo costante sulle procedure per il salvataggio dei dati, attraverso l'outsourcer, al fine di consentire il corretto e tempestivo ripristino in caso di perdita di integrità delle informazioni o di danneggiamento.

Responsabili o consulenti esterni da contattare in caso di emergenza:

- Byte Wise S.r.l. con sede a Roma nella via A. Ravà n. 106, t. 06.54225477, mob. 389 6440040 (Responsabile IT)

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

4. PROCEDURA PER LA GESTIONE DELLE RICHIESTE DEGLI INTERESSATI

In relazione al trattamento dei dati personali, è assicurato agli interessati l'effettivo esercizio dei propri diritti. Le istanze possono essere trasmesse al titolare del trattamento (mediante lettera raccomandata all'indirizzo della fondazione – via G. Reni 4/A – 00196 Roma - o mediante email all'indirizzo privacy@fondazionemaxxi.it) che dovrà provvedere entro e non oltre trenta giorni. In ogni caso, l'interessato potrà presentare reclamo all'Autorità Garante per la protezione dei dati personali.

Nel caso di richiesta di accesso ai propri dati, l'interessato potrà ricevere una copia dei suoi dati personali e le seguenti informazioni:

- le finalità del trattamento
- le categorie dei dati personali interessate
- i destinatari o le categorie di destinatari ai quali i dati sono stati diffusi
- se possibile, il tempo previsto per il quale i dati personali sono memorizzati o i criteri usati per determinare questo tempo
- se i dati personali non sono stati raccolti presso l'interessato, eventuali informazioni disponibili sulla fonte delle informazioni
- l'esistenza di processi decisionali automatizzati
- se i dati sono trasferiti in altre nazioni e quali misure sono state messe in atto.

La richiesta dovrà essere scritta e corredata della fotocopia del proprio documento di identità.

L'addetto autorizzato al trattamento sarà tenuto ad accertare l'effettiva esistenza dei dati personali e di ciò si darà comunicazione al richiedente mediante email. L'utilizzo di altri mezzi di comunicazione (ad esempio, lettera) sarà subordinato al pagamento delle spese del servizio adoperato, da parte dell'interessato, il quale verrà informato dei suddetti costi. La risposta alla richiesta di accesso ai dati deve essere inoltrata entro 30 giorni dalla ricezione.

Nel caso di richiesta di rettifica dei propri dati, l'interessato dovrà comunicare alla Fondazione le eventuali informazioni incomplete che lo riguardano. La richiesta verrà inoltrata all'addetto autorizzato al trattamento, il quale provvederà alla correzione. Di ciò si darà comunicazione all'interessato mediante email. L'utilizzo di altri mezzi di comunicazione (ad esempio, lettera) sarà subordinato al pagamento delle spese del servizio adoperato, da parte dell'interessato, il quale verrà informato dei suddetti costi.

Nel caso di richiesta di eliminazione dei dati personali, la Fondazione valuterà se i dati personali non sono più necessari in relazione alla finalità per i quali sono stati originariamente raccolti o altrimenti trattati. Se il trattamento è basato sul consenso, l'interessato dovrà ritirare il proprio consenso: in tal caso, se non vi sono altri fondamenti legali per continuare a trattari i dati l'addetto autorizzato al trattamento procederà alla cancellazione. Se l'interessato si è opposto al trattamento e non vi sono motivi legittimi fondati per il trattamento, o se i dati sono stati trattati illegalmente, se i dati devono essere cancellati per conformarsi ad obblighi legali o sono stati raccolti per offrire servizi in ambito ICT, la Fondazione, senza ritardo, procede alla cancellazione.

Nel caso di richiesta di limitazione dei dati, la Fondazione procede senza ritardo qualora ricorrono le seguenti condizioni:

- l'accuratezza dei dati personali è stata contestata dall'interessato, per il periodo che consente al titolare di verificare l'esattezza dei dati

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

- il trattamento è illegale e l'interessato si oppone alla cancellazione dei dati e richiede invece la limitazione del suo utilizzo
- il titolare o il responsabile non hanno più bisogno dei dati ai fini del trattamento, ma la restrizione è richiesta dall'interessato per l'esercizio o la difesa di diritti
- l'interessato ha obiettato al trattamento e la restrizione rimane in sospeso in attesa di verificare se i motivi legittimi del titolare o responsabile prevalgono su quelli dell'interessato

La richiesta verrà inoltrata all'addetto autorizzato al trattamento, il quale provvederà alla limitazione. Di ciò si darà comunicazione all'interessato mediante email. L'utilizzo di altri mezzi di comunicazione (ad esempio, lettera) sarà subordinato al pagamento delle spese del servizio adoperato, da parte dell'interessato, il quale verrà informato dei suddetti costi.

Quando l'interessato esercita il diritto alla portabilità dei dati e chiede che le informazioni siano trattate con sistemi ICT, l'addetto autorizzato al trattamento, se del caso insieme al responsabile ICT della Fondazione, verifica che l'interessato sia in grado di ricevere tali dati o di trasmetterli ad altro soggetto. Pertanto, la Fondazione fornisce all'interessato o ad altro soggetto da questi nominato, con un formato strutturato, comunemente usato, leggibile da una macchina e a titolo gratuito i dati richiesti.

Nel caso di opposizione al trattamento dei dati, l'interessato dovrà specificare i dati personali dei quali si oppone al trattamento. La richiesta verrà gestita dall'addetto autorizzato al trattamento, verificando che il trattamento sia cessato e non vi sia altro obbligo per la prosecuzione. Di ciò si darà comunicazione all'interessato mediante email. L'utilizzo di altri mezzi di comunicazione (ad esempio, lettera) sarà subordinato al pagamento delle spese del servizio adoperato, da parte dell'interessato, il quale verrà informato dei suddetti costi.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

5. PROCEDURA PER LA VIOLAZIONE DEI DATI (data breach)

La Fondazione MAXXI procede, secondo le modalità previste dall'art. 33, n. 3 Regolamento (UE) n. 2016/679, alla notifica dell'eventuale violazione dei dati personali, della quale è venuta a conoscenza direttamente o su informazione del Responsabile del trattamento, all'Autorità Garante per la protezione dei dati personali (o all'Autorità di Controllo competente), a meno che il rischio derivante dalla violazione per i diritti e le libertà dell'interessato venga valutato come improbabile.

La Fondazione detiene adeguata e completa documentazione di qualsiasi violazione, al fine di consentire all'Autorità di controllo di verificare la conformità del trattamento alla normativa vigente. La documentazione è detenuta presso l'area gestione risorse umane e affari legali o presso altra area appositamente individuata.

Qualsiasi addetto al trattamento dei dati che viene a conoscenza di una violazione deve darne comunicazione immediata al Responsabile della protezione dei dati, all'Amministratore di sistema e al Referente dell'area gestione risorse umane e affari legali, affinchè si proceda all'adozione di tutte le misure necessarie per il ripristino delle informazioni e per porre rimedio alla violazione.

Il Responsabile della protezione dei dati, l'Amministratore di sistema e il Responsabile dell'Ufficio Legale devono essere preparati a rispondere a una violazione dei dati personali effettiva o presunta, 24 ore su 24, 7 giorni su 7, per tutto l'anno. Le informazioni di contatto di ciascuno di loro devono essere archiviate in un sito centrale e devono essere utilizzati per riunirli ogni volta che viene ricevuta una notifica di effettiva o presunta violazione dei dati. Il gruppo può scegliere di avvalersi di personale aggiuntivo o di consulenti esterni allo scopo di gestire la violazione dei dati.

Una volta comunicata la violazione, il gruppo si riunisce (anche attraverso strumenti telematici) per:

- assegnare un livello di urgenza alla violazione dei dati personali
- avviare al più presto una indagine
- individuare i requisiti per la risoluzione e monitorare la soluzione
- riferire i risultati alla Governance della Fondazione
- coordinare le comunicazioni interne ed esterne
- documentare tutte le decisioni assunte

La Fondazione comunicherà, attraverso i propri canali di contatto (email, lettera, etc…), la violazione dei dati personali anche agli interessati, nel caso in cui questa presenta rischi elevati per i diritti e le libertà degli interessati e salvo che non ricorrano le condizioni previste dall'art. 34, n. 3 del Regolamento (UE) n. 2016/679. Tale comunicazione potrà avvenire contestualmente alla notifica e dovrà contenere le informazioni di seguito indicate: contatti del Responsabile della protezione dei dati (DPO); le conseguenze probabili della violazione in questione; le misure adottate o da adottare per porre rimedio alla violazione.

Qualora la violazione riguarda i dati personali che vengono elaborati dalla Fondazione per conto di terzi, il Responsabile della protezione dei dati deve segnalare qualsiasi violazione dei dati al rispettivo titolare, senza indebito ritardo. Il Responsabile della protezione dei dati invierà al titolare una notifica che contiene le seguenti informazioni:

- una descrizione della natura della violazione
- le categorie di dati personali coinvolti
- il numero approssimativo degli interessati coinvolti

- il nome e le informazioni di contatto del Responsabile della Protezione dei dati, del referente dell'area gestione risorse umane e affari legali e dell'Amministratore di sistema
- le conseguenze della violazione dei dati personali
- le misure adottate per gestire la violazione
- qualsiasi altra informazione relativa alla violazione.

Qualsiasi soggetto che viola la procedura suddetta sarà soggetto a misure disciplinari interne.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale
delle arti del XXI secolo

6. NON CONFORMITA' E AZIONI CORRETTIVE

Quando si verifica una non conformità ai requisiti legali di riferimento, la Fondazione MAXXI reagisce alla non conformità e, per quanto applicabile, intraprende tutte le azioni possibili per tenerla sotto controllo e correggerla e ne affronta le conseguenze. La Fondazione valuta, altresì, l'esigenza di avviare altre azioni per eliminare le cause della non conformità, in modo che non si ripeta o non si verifiche altrove, riesaminando e analizzando la non conformità, determinando le cause della non conformità, determinando se esistono o potrebbero verificarsi non conformità simili. Se applicabile, la Fondazione comunica la violazione dei dati personali all'interessato e all'Autorità di controllo, con le modalità previste nel presente Regolamento. Infine, la Fondazione effettua, ove necessario, le modifiche alle misure di protezione dei dati personali.

Della natura della non conformità, delle azioni intraprese e dei risultati raggiunti viene conservata la documentazione.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale
delle arti del XXI secolo

7. AGGIORNAMENTO POSIZIONI

La Fondazione MAXXI aggiorna tutte le posizioni di chi effettua un trattamento dei dati personali, in virtù dei cambiamenti interni all'organizzazione e ai mutati rapporti con terze parti. In particolar modo queste ultime devono essere identificate come titolari autonomi, contitolari o responsabili del trattamento prima di effettuare qualsiasi operazione sui dati personali.

L'aggiornamento viene effettuato generalmente ogni anno o comunque all'occorrenza, allorquando vengono stipulati nuovi contratti di lavoro o di consulenza con gli outsourcers.

Gli accordi e gli atti giuridici con sui sono regolati i rapporti con l'organizzazione con i contitolari o i responsabili del trattamento vengono conservati presso l'Area gestione delle risorse umane e degli affari legali.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale
delle arti del XXI secolo

8. CONTRATTI E BANDI

La Fondazione MAXXI raccomanda di inserire nei contratti e nei bandi per la fornitura di beni o servizi un articolato o clausola privacy relativa al trattamento dei dati personali richiesti. A tal fine si riporta il testo che potrebbe essere adottato:

"*I dati personali raccolti sono trattati in osservanza del Regolamento UE n. 2016/679 e della normativa vigente in materia di trattamento dei dati personali e di libera circolazione di tali dati, per quanto è necessario all'esecuzione del contratto/rapporto e per adempiere agli obblighi di legge alle quali la Fondazione MAXXI soggiace. Nel momento in cui i dati personali sono ottenuti, la Fondazione MAXXI adotta le misure necessarie per garantire un trattamento lecito, corretto e trasparente delle informazioni. Per ulteriori specificazioni si rinvia all'informativa sul trattamento dei dati personali ex artt. 13-14 Reg.to UE 2016/679 allegata al presente contratto* […]

La Parte dichiara di avere ricevuto l'informativa di cui agli artt. 12 e 13 del Regolamento UE 2016/679 e di acconsentire al trattamento dei dati personali ad opera della Fondazione MAXXI, dei suoi collaboratori, sostituti e/o addetti (delegati etc).

Luogo e Data

La Parte"

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

9. VIDEOSORVEGLIANZA

I dati vengono raccolti esclusivamente mediante riprese videoregistrate che, in relazione ai luoghi di installazione delle videocamere, interessano prevalentemente i soggetti e i mezzi di trasporto eventuali che transitano nell'area interessata.

a. Finalità del trattamento

La videosorveglianza è utilizzata per la protezione e l'incolumità, interna ed esterna agli edifici ove si svolgono le attività e i servizi, degli individui e dei beni aziendali. In ogni caso, è fatto salvo il trattamento dei dati personali per ottemperare alle esigenze attinenti alla prevenzione, all'accertamento e alla repressione dei reati commessi, alla sicurezza pubblica, all'esercizio del diritto di difesa del titolare o di terzi, in ogni sede giudiziaria, sulla base delle immagini captate dalle videocamere (acquisizione di prove).

Tutte le telecamere del sistema di videosorveglianza in uso presso la Fondazione MAXXI, sia quelle perimetrali che riprendono le aree esterne del Museo, della biblioteca e degli Uffici Amministrativi, sia quelle interne, sono utilizzate per garantire la sicurezza dei beni rispetto a danneggiamenti, atti di vandalismo, sicurezza del lavoro, furti, aggressioni, rapine, e fatti analoghi.

In generale, tutte le telecamere, sia esterne che interne, sono volte a:

- Accertare e contestare comportamenti illeciti qualora essi avvengono in aree esterne o interne sottoposte a controllo, sia in orari notturni che diurni.
- Agevolare l'attività di indagine dell'Autorità Giudiziaria o le indagini difensive, attraverso l'acquisizione delle immagini captate attraverso il sistema di videosorveglianza, al fine di accertare la commissione di atti illeciti o presunti tali.

Nello specifico, tutte le telecamere, sia esterne che interne, sono volte a:

- Prevenire accessi non autorizzati e altri comportamenti illeciti attraverso un effetto deterrente che il sistema di videosorveglianza è in grado di produrre nell'area pubblica della piazza Alighiero Boetti e delle zone limitrofe, negli spazi espositivi del Museo e all'interno della Biblioteca e accessi caffetteria/sale espositive.
- Sorvegliare gli spazi museali e le aree esterne che in occasione di eventi a partecipazione pubblica o di rilevante importanza possono presentare elementi di criticità, anche sotto il profilo dell'ordine pubblico.
- Proteggere l'integrità del notevole patrimonio mobiliare e immobiliare della Fondazione MAXXI da atti vandalico e da danneggiamenti di terzi.

b. Legittimo interesse della Fondazione MAXXI

Le finalità perseguite attraverso il sistema di videosorveglianza soddisfano il legittimo interesse della Fondazione MAXXI contro i rischi di comportamenti illeciti o presunti tali.

In particolare, si segnala il valore assicurativo complessivo delle Collezioni di opere d'arte della Fondazione MAXXI, pari ad euro38.204.433,48, così suddivisi come da nota prot. N. 2518U del 22/11/2019, allegata alla presente. La Fondazione MAXXI assicura peraltro le opere presenti nelle esposizioni temporanee: nel primo decennio di attività, il valore massimo assicurato è stato stimato in euro 18.760.000.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

Necessità del trattamento

Il sistema di videosorveglianza comporta esclusivamente il trattamento delle immagini rilevate mediante le riprese video e che, in relazione ai luoghi di installazione delle videocamere, interesseranno i soggetti e i mezzi di trasporto che transitano o sostano nell'area videosorvegliata.

L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando, quando non indispensabile, immagini dettagliate o ingrandite non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza. Nel caso di videocamere che riprendono le aree perimetrali esterne degli edifici della Fondazione, l'angolo di visuale è delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti gli edifici.

Il trattamento è effettuato senza ledere i diritti e le libertà degli interessati, con particolare riferimento alla riservatezza e all'identità personale.

Nell'attività di videosorveglianza è infatti rispettato il divieto di controllo a distanza dell'attività lavorativa, ai sensi dell'art. 4 dello Statuto dei lavoratori: non sono installate apparecchiature specificamente preordinate alla predetta finalità. In ogni caso, l'accordo sindacale stipulato dalla Fondazione MAXXI, ai sensi della normativa di settore, protegge e garantisce i dipendenti della Fondazione.

La disponibilità in tempo reale delle immagini costituisce uno strumento di prevenzione e dissuasione e garantisce altresì un intervento immediato del personale di sicurezza.

D'altro canto, la memorizzazione delle immagini, soprattutto durante gli orari notturni o in aree non raggiunte dal personale di sicurezza, consente altresì la conservazione di mezzi di prova per l'accertamento di comportamenti illeciti.

Unitamente alla videosorveglianza sono previsti altri sistemi di controllo che, tuttavia, non consentono di perseguire le finalità di sicurezza e protezione del Museo.

In particolare, il servizio di guardiania fisica è previsto all'ingresso del Museo, sul varco antistante la via G. Reni n. 4/A; gli altri varchi di accesso alla Fondazione MAXXI non sono controllati dal servizio di guardiania. Inoltre, il servizio non è assicurato durante gli orari notturni.

Il servizio di guardiania fisica è previsto anche all'ingresso del Museo MAXXI L'Aquila, in piazza Santa Maria Paganica; il servizio non è assicurato durante gli orari notturni.

Il servizio di guardiania fisica è previsto all'interno di Casa Balla; il servizio non è assicurato durante gli orari notturni o di chiusura al pubblico. È previsto un impianto antitrusione.

Il sistema di recinzione degli spazi non costituisce un valido deterrente contro gli accessi non autorizzati al Museo, soprattutto in orario notturno.

Il Museo della sede de L'Aquila non ha un sistema di recinzione degli spazi esterni.

Casa Balla si trova all'interno di un edificio adibito a civili abitazioni con accesso da un androne comune.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

In considerazione del valore assicurativo delle Collezioni, il sistema di videosorveglianza anche all'interno degli spazi museali è reso necessario, giacchè il personale di sala non può controllare tutte le aree espositive.

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Collocazione server

I dati personali oggetto del trattamento sono custoditi nel server situato presso la Control Room della Sede di Roma della Fondazione MAXXI. L'ufficio è ubicato all'ingresso principale del Museo MAXXI di Roma, in luogo chiuso e non accessibile al pubblico.

La sede dell'Aquila del Museo MAXXI dispone di una Control Room all'interno della quale sono collocati i gli schermi e di un locale tecnico separato, all'interno del quale si trovano i server. I locali non sono accessibili al pubblico. L'accesso alle immagini può avvenire anche da remoto presso la Sede di Roma della Fondazione, attraverso strumenti collocati nella Control Room: l'accesso a tali immagini avviene soltanto da parte del Titolare del trattamento o da suo delegato.

Casa Balla non dispone di una Control Room interna. I dati personali oggetto del trattamento sono custoditi nel server situato presso la Control Room della Sede di Roma della Fondazione MAXXI.

Autorizzazioni

L'accesso ai locali ove è custodito il server è consentito solamente alle persone fisiche, incaricate del trattamento, autorizzate, per iscritto, ad utilizzare gli impianti e a visionare le registrazioni. In particolare, autorizzata dal Titolare ad accedere agli impianti e al trattamento delle immagini videoregistrate è il Responsabile dell'Ufficio Tecnico; anche il personale addetto alla videosorveglianza è autorizzato ad utilizzare gli impianti; il personale incaricato della manutenzione del server è autorizzato ad accedere al sistema. Eventuali accessi di persone diverse da quelle innanzi indicate (come, a mero titolo esemplificativo, il personale addetto alla pulizia dei locali) devono essere autorizzato, per iscritto, dal Titolare del trattamento.

Il Titolare del trattamento designa e nomina gli addetti autorizzati alla gestione del servizio di videosorveglianza nell'ambito dei propri dipendenti e di aziende esterne debitamente nominate, se del caso, quali responsabili del trattamento che, per capacità, affidabilità ed esperienza forniscono idonea garanzia nel rispetto della normativa vigente in materia di protezione dei dati personali.

Possono essere autorizzati all'accesso alla control room solo gli addetti autorizzati per gli scopi connessi alle finalità di cui al presente Regolamento, nonché il personale addetto alla manutenzione degli impianti e alla pulizia dei locali, i cui nominativi dovranno essere comunicati per iscritto al Titolare del trattamento. Il Titolare del trattamento impartisce adeguate istruzioni atte ad evitare il rilevamento di dati da parte delle persone autorizzate ad accedere ai locali per la manutenzione degli impianti e alla pulizia dei locali.

L'accesso al server è esclusivamente consentito al Titolare del trattamento, agli addetti autorizzati e al personale addetto alla manutenzione, con le modalità prescritte dal presente Regolamento.

Gli addetti autorizzati al trattamento saranno dotati di password di accesso al sistema. Il sistema dovrà essere fornito di log di accesso che saranno conservati per la durata di 1 mese, fatti salvi tempi diversi di conservazione in base a specifiche esigenze.

Collocazione monitor

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

I monitor degli impianti di videosorveglianza sono allocati in modo tale da non permettere la visione delle immagini, neppure occasionalmente, a persone estranee non autorizzate ad accedere alla control room.

Accesso alle immagini

L'accesso alle immagini da parte degli addetti autorizzati al trattamento, si limita alle attività oggetto della sorveglianza; eventuali altri informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione. Nel caso le immagini siano conservate, i relativi supporti vengono custoditi, per l'intera durata della conservazione, in un armadio o struttura simile dotata di serratura, apribile solo dagli addetti autorizzati al trattamento. La cancellazione delle immagini sarà garantita mediante gli strumenti e le procedure più adeguate.

Fatti salvi i casi di richieste degli interessati, i dati registrati possono essere riesaminati, nel limite di tempo ammesso per la conservazione, solo in caso di effettiva necessità per il conseguimento delle finalità predette e a seguito di regolare autorizzazione richiesta al Titolare.

Modalità di accesso alle immagini

In caso di rilevazione di immagini di fatti concernenti ipotesi di reato, commessi all'interno dei locali della Fondazione e/o del Museo, ovvero negli spazi esterni circostanti, per la tutela del patrimonio aziendale o dei beni, propri o altrui, collocati all'interno degli spazi aziendali (come, a titolo meramente esemplificativo, nel caso di danneggiamento di opere o beni aziendali, sottrazione di beni, anomalie di funzionamento, etc) o per la salvaguardia della incolumità fisica delle persone, ovvero nei casi di fatti concernenti ipotesi di reato, commessi all'esterno del perimetro della Fondazione e/o del Museo di cui la Fondazione ha avuto immediata conoscenza, il Titolare del trattamento, o un suo delegato, o il Responsabile dell'Ufficio Tecnico, in casi indifferibili e urgenti, provvederà a darne comunicazione senza ritardo alle Forze dell'ordine o all'Autorità competente, provvedendo, nel contempo, alla conservazione delle immagini su appositi supporti. Alle immagini raccolte ai sensi del presente articolo possono accedere soltanto gli appartenenti alla Autorità e/o alla polizia giudiziaria, le persone da essi autorizzate, il Responsabile dell'Ufficio Tecnico nonché il Titolare del trattamento o persona da essa espressamente delegata.

Quando non ricorrono ipotesi indifferibili e urgenti di accesso alle immagini, e nello svolgimento dei normali compiti istituzionali, le Forze dell'ordine o l'Autorità Giudiziaria possono presentare istanza scritta e motivata al Titolare del trattamento per chiedere copia delle riprese effettuate. Analoga richiesta, per la tutela giudiziaria di diritti, può essere presentata per iscritto e motivata, dai soggetti autorizzati allo svolgimento di indagini difensive. Il Titolare del trattamento, previa valutazione dell'istanza, potrà autorizzare la visione delle immagini, indicando le specifiche modalità. In ogni caso, la rilevazione e l'accesso alle immagini viene effettuata dal personale espressamente autorizzato dal Titolare del trattamento e/o dal Responsabile dell'Ufficio Tecnico, il quale provvede, nel contempo, alla conservazione delle immagini su appositi supporti

Quando non rilevano immediatamente ipotesi di reato, per la tutela del patrimonio aziendale o dei beni, propri o altrui, collocati all'interno degli spazi aziendali, (come, a titolo meramente esemplificativo, nel caso di danneggiamento di opere o beni aziendali, sottrazioni di beni, anomali di funzionamento, etc), o per la salvaguardia della incolumità fisica delle persone, il personale della Fondazione può chiedere l'accesso alle immagini, formulando un'istanza tramite il Responsabile della propria Area di appartenenza e indirizzata al Segretario Generale il quale, previa valutazione, potrà autorizzare la visione delle immagini, indicando le

specifiche modalità. In ogni caso, la rilevazione e l'accesso alle immagini viene effettuata dal personale espressamente autorizzato dal Titolare del trattamento e/o dal Responsabile dell'Ufficio Tecnico, il quale provvede, nel contempo, alla conservazione delle immagini su appositi supporti.

Nelle ipotesi di cui sopra, terzi possono presentare una richiesta scritta e motivata al Titolare del trattamento, il quale, previa valutazione dell'istanza, potrà autorizzare la visione delle immagini, indicandone le specifiche modalità. In ogni caso, la rilevazione e l'accesso alle immagini viene effettuata dal personale espressamente autorizzato dal Titolare del trattamento e/o dal Responsabile dell'Ufficio Tecnico, il quale provvede, nel contempo, alla conservazione delle immagini su appositi supporti.

Infine, nell'eventualità in cui si rende necessaria una modifica del puntamento di una o più telecamere, tale necessità viene segnalata espressamente al Segretario Generale dai Direttori dei Dipartimenti che, oltre ad indicare le ragioni, le modalità e i tempi della modifica, individuano anche il personale espressamente incaricato a regolare il puntamento. Il Segretario Generale autorizza il personale suddetto ad effettuare la modifica. La modifica del puntamento viene effettuato con l'ausilio del personale dell'Ufficio tecnico preposto alla gestione del sistema di videosorveglianza, avendo cura di annotare in apposito registro, tra le altre cose, le modifiche effettuate, i tempi e le finalità del nuovo puntamento.

Tutti gli accessi alla visione saranno documentati mediante annotazione in un apposito registro (cartaceo e/o informatico), conservato nei locali server, nel quale sono riportati:

- data e ora di accesso
- i dati personali per i quali si è svolto l'accesso
- la motivazione dell'autorizzazione all'accesso
- i terzi autorizzati

Informazioni per gli interessati

Gli interessati devono essere informati che stanno per accedere ad una zona videosorvegliata. In osservanza del provvedimento in materia di videosorveglianza reso dall'Autorità Garante per la protezione dei dati personali l'8 aprile 2010, possono essere installati uno o più cartelli, in relazione alla presenza di una o più telecamere e secondo il loro raggio di azione.

Tali cartelli possono essere collocati in modo da essere ben visibili in ogni condizione di illuminazione ambientale; inglobano un simbolo o una stilizzazione di esplicita e immediata comprensione; sono allocati prima della zona videosorvegliata, anche nelle immediate vicinanze della telecamera.

In ogni caso, fatte salve le ipotesi di liceità del trattamento per la salvaguardia di interessi vitali dell'interessato o di altre persone fisiche, per l'esercizio di un compito di interesse pubblico, o per adempiere ad un obbligo di legge, l'informativa viene resa disponibile all'interessato in modo agevole e senza oneri (anche mediante affissione in bacheche o locali, avvisi, carelli agli sportelli per gli utenti).

MODALITA' DI RACCOLTA, CONSERVAZIONE E REQUISITI DEI DATI PERSONALI

I dati personali vengono trattati in modo lecito e secondo correttezza per le finalità indicate nel presente Regolamento.

I dati vengono trattati in modo pertinente, completo e non eccedente, rispetto alle finalità per le quali sono raccolti e successivamente trattati.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

I dati vengono conservati per un periodo di tempo non superiore a quello strettamente necessario al soddisfacimento delle finalità dell'impianto, per le quali essi sono raccolti e successivamente trattati e, in ogni caso, per un periodo di tempo non superiore alle 96 ore successive alla rilevazione, per esigenze di tutela e conservazione delle opere d'arte presenti nel Museo. In ogni caso, sono fatte salve speciali esigenze di ulteriore conservazione in relazione a festività, chiusura del Museo o degli Uffici della Fondazione, o per aderire ad una richiesta della Polizia Giudiziaria o dell'Autorità Giudiziaria.

I dati vengono trattati con modalità idonee a salvaguardare l'anonimato, anche successivamente alla raccolta.

Non sono consentite riprese di dettaglio dei tratti somatici delle persone fisiche, che non siano funzionali alle finalità istituzionali dell'impianto attivato. Le telecamere presentano le caratteristiche descritte in un'apposita relazione rilasciata dalla ditta installatrice e tale materiale è conservato a cura del Titolare.

DIRITTI DEGLI INTERESSATI

In relazione al trattamento dei dati personali, è assicurato agli interessati l'effettivo esercizio dei propri diritti. Le istanze possono essere trasmesse al titolare del trattamento mediante lettera raccomandata o pec, che dovrà provvedere entro e non oltre trenta giorni. In ogni caso, l'interessato potrà presentare reclamo all'Autorità Garante per la protezione dei dati personali.

Nel caso di richiesta di accesso ai propri dati, l'interessato potrà avere visione soltanto delle immagini che lo riguardano direttamente. La richiesta dovrà essere motivata, quanto più possibile precisa, scritta e corredata della fotocopia del proprio documento di identità. L'istanza deve indicare a quale impianto di sorveglianza si fa riferimento e il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di ripresa.

Il Titolare del trattamento, previa valutazione dell'istanza, potrà autorizzare la visione delle immagini, indicandone le specifiche modalità.

Il Responsabile dell'Ufficio tecnico sarà tenuto ad accertare l'effettiva esistenza delle immagini e alla conservazione delle immagini su appositi supporti; di ciò darà comunicazione al richiedente. Nel caso di accertamento positivo, verrà fissato il giorno, l'ora e il luogo in cui l'interessato potrà visionare le immagini che lo riguardano. La risposta alla richiesta di accesso ai dati deve essere inoltrata entro 30 giorni dalla ricezione.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

10. FORMAZIONE

La Fondazione Maxxi cura che i propri dipendenti, autorizzati al trattamento dei dati personali, siano debitamente formati. Pertanto, viene annualmente progettato un piano di formazione per gli addetti al trattamento.

Quando si procede alla nomina di un nuovo incaricato, è prevista la seguente formazione:

- comunicazione scritta delle istruzioni complete dell'ambito di trattamento al quale è proposto il nuovo incaricato e formazione orale sugli obblighi di legge e le norme di condotta da parte del titolare o del Responsabile della protezione dei dati.

Quando si procede al mutamento delle mansioni, è prevista la seguente formazione:

- assegnazione di istruzioni scritte complete relative al nuovo trattamento.

Il mancato svolgimento degli obblighi formativi può comportare l'applicazione di sanzioni disciplinari.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

MAXXI Museo nazionale delle arti del XXI secolo

11. LINEE GUIDA PER IL TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI IN AMBITO LAVORATIVO

Le presenti prescrizioni specifiche non pregiudicano l'applicazione delle disposizioni di legge e delle norme interne alla Fondazione, vigenti in materia di trattamento e protezione dei dati personali, e sono adottate in seguito al Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 , n. 146 del 5 giugno 2019 emesso dall'Autorità Garante per la Protezione dei Dati Personali.

Le linee guida si applicano ai dati personali delle seguenti categorie di interessati:

- Candidati all'instaurazione dei rapporti di lavoro, anche in caso di curricula spontaneamente trasmessi dagli interessati

- Lavoratori subordinati, anche se parti di un contratto di apprendistato, di formazione, a termine, di lavoro intermittente, di lavoro occasionale, ovvero prestatori di lavoro nell'ambito di un contratto di somministrazione di lavoro, o in rapporto di tirocinio o di volontariato

- Consulenti e liberi professionisti

- Altri lavoratori autonomi in rapporto di collaborazione

- Persone fisiche che ricoprono cariche sociali o altri incarichi nell'Associazione

- Terzi danneggiati nell'esercizio dell'attività lavorativa o professionale dai soggetti di cui sopra

- Terzi (familiari o conviventi dei soggetti di cui sopra) per il rilascio di agevolazioni e permessi

Il regolamento ha ad oggetto: dati personali, particolari categorie di dati personali, dati giudiziari

Il trattamento dei dati è effettuato solo se necessario per le seguenti esigenze:

- Per adempiere o esigere l'adempimento di obblighi di legge o di contratti collettivi anche aziendali ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, del riconoscimento di agevolazioni, dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza e assistenza anche integrativa, in materia di igiene e sicurezza del lavoro, in materia fiscale e sindacale

- Per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di salute e sicurezza del lavoro e di malattie professionali o per danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale

- Per garantire le pari opportunità nel lavoro

- Per perseguire scopi determinati e legittimi individuati dallo Statuto della Fondazione

Trattamenti effettuati nella fase preliminare all'assunzione:

- La Fondazione può trattare i dati idonei a rilevare lo stato di salute e l'origine razziale ed etnica dei candidati all'instaurazione di un rapporto di lavoro o di collaborazione, solo se la raccolta è giustificata da scopi determinati e legittimi ed è necessaria per instaurare tale rapporto.

- Nel caso in cui siano i candidati a fornire particolari categorie di dati, di propria iniziativa, in particolare attraverso l'invio di curricula, il trattamento deve riguardare le sole informazioni strettamente pertinenti e limitate a quanto necessarie a tali finalità, tenendo conto anche delle mansioni o dei profili

professionali richiesti. Qualora nei curricula inviati dai candidati siano presenti dati non pertinenti rispetto alla finalità perseguita, la Fondazione deve astenersi dall'utilizzare tali informazioni.

- I dati genetici non possono essere trattati al fine di stabilire l'idoneità professionale di un candidato all'impiego, neppure con il consenso.

- I curricula dei candidati non selezionati vanno conservati soltanto per il tempo necessario per la selezione, successivamente vanno eliminati fisicamente e digitalmente. I curricula dei candidati selezionati possono essere trasmessi soltanto agli Uffici direttamente interessati al profilo professionale del candidato.

- Con riguardo alla pubblicità degli esiti delle graduatorie finali delle selezioni o di altri procedimenti che prevedono la formazione di graduatorie, devono essere diffusi i soli dati pertinenti e non eccedenti riferiti agli interessati (ad esempio, non possono essere pubblicati i recapiti riferiti a utenze fisse o mobili, l'indirizzo di residenza o di posta elettronica, il codice fiscale, l'indicatore isee, il numero di figli disabili, i risultati di test psicoattitudinali o i titoli di studio), né possono essere diffusi i dati concernenti le condizioni di salute degli interessati, ivi compresi i riferimenti a condizioni di invalidità, disabilità o handicap fisici e/o psichici. Al fine poi di agevolare le modalità di consultazione delle graduatorie oggetto di pubblicazione, possono essere messe a disposizione degli interessati in aree ad accesso selezionato dei siti web istituzionali consentono la consultazione degli esiti delle prove o del procedimento ai soli partecipanti alla procedura selettiva mediante l'attribuzione agli stessi di credenziali di autenticazione (username, password, numero di protocollo o altri estremi identificativi).

Trattamenti di particolari categorie di dati effettuati nel corso del rapporto di lavoro:

- La Fondazione tratta i dati che rivelano le convinzioni religiose o filosofiche ovvero l'adesione ad associazioni o organizzazioni a carattere religioso o filosofico esclusivamente in caso di fruizione di permessi in occasione di festività religiose o per l'esercizio dell'obiezione di coscienza.

- La Fondazione tratta i dati che rivelano le opinioni politiche o l'appartenenza sindacale, o l'esercizio di funzioni pubbliche e incarichi politici, di attività o di incarichi sindacali esclusivamente ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali nonché per consentire l'esercizio dei diritti sindacali compreso il trattamento dei dati inerenti alle trattenute per il versamento delle quote di iscrizione ad associazioni od organizzazioni sindacali.

- La Fondazione tratta i dati che rilevano lo stato di salute al fine della fruizione di permessi, del godimento di benefici di legge, quando è strettamente necessario per l'assegnazione di mansioni. Quando il lavoratore fornisce spontaneamente documenti che contengono dati sanitari, l'Ufficio HR tratta soltanto le informazioni necessarie e indispensabili al riconoscimento dei benefici, astenendosi dall'utilizzare le informazioni non pertinenti.

- In caso di partecipazione ad operazioni elettorali in qualità di rappresentante di lista, l'Ufficio HR non deve trattare dati che rilevino le opinioni politiche, nell'ambito della documentazione da presentare al fine del riconoscimento dei benefici di legge.

- La Fondazione non può trattare dati genetici al fine di stabilire l'idoneità professionale di un dipendente, neppure con il suo consenso.

Modalità di comunicazione dei dati:

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

- In tutte le comunicazioni all'interessato che contengono categorie particolari di dati devono essere utilizzate forme di comunicazione anche elettroniche individuali nei confronti di quest'ultimo o di un suo delegato. Nel caso si proceda alla trasmissione del documento cartaceo, questo dovrà essere trasmesso, di regola, in plico chiuso, salva la necessità di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto.

- Per ragioni specificamente indicate dagli Uffici richiedenti, l'Ufficio competenti a gestire le risorse umane trasmettono loro i dati personali, attraverso documenti che devono contenere esclusivamente le informazioni necessarie allo svolgimento della funzione, senza allegare, ove non strettamente indispensabile, documentazione integrale, o riportare stralci all'interno del testo.

Di norma, gli Uffici competenti a gestire le risorse umane trasmette i dati personali trattati agli Uffici competenti, per le seguenti finalità:

- Per la tenuta della contabilità e per la corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori

- Per perseguire finalità di salvaguardia della vita o dell'incolumità fisica del lavoratore o di un terzo

- Per far valere o difendere un diritto, anche da parte di un terzo, in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione. Il trattamento dei dati personali effettuato per la presente finalità deve riferirsi a contenziosi in atto o a situazioni precontenziose.

- Quando per ragioni di organizzazione del lavoro, e nell'ambito della predisposizione di turni di servizio, si proceda a mettere a disposizione a soggetti diversi dall'interessato (altri colleghi), dati relativi a presenze ed assenze dal servizio, la Fondazione non deve esplicitare, nemmeno attraverso acronimi o sigle, le causali dell'assenza dalle quali sia possibile evincere la conoscibilità di particolari categorie di dati personali (es. permessi sindacali o dati sanitari).

Responsabili del trattamento:

- Ai fini del trattamento dei dati personali, la Fondazione può trasmettere i dati dei lavoratori a figure soggettive esterne, appositamente nominate quali responsabili del trattamento, che, a diverso titolo, possono trattare questi dati.

Misure di sicurezza specifiche:

- La Fondazione provvede a conservare separatamente da ogni altro dato personale dell'interessato le informazioni che contengono categorie particolari di dati, utilizzando sezioni del fascicolo personale cartaceo appositamente dedicate alla custodia dei dati particolari, inclusi quelli idonei a rivelare lo stato di salute del lavoratore, da conservare separatamente e in modo da non consentirne una indistinta consultazione nel corso delle ordinarie attività amministrative. Nel caso in cui i lavoratori producono spontaneamente certificati medici, la Fondazione deve adottare gli opportuni accorgimenti per non rendere visibili le diagnosi contenute nei certificati (ad esempio, prescrivendone la circolazione in busta chiusa previo oscuramente di tali informazioni); ciò, al fine di impedire ogni accesso abusivo a tali dati da parte di soggetti non designati come addetti al trattamento.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale
delle arti del XXI secolo

- La Fondazione garantisce che i luoghi ove si svolge il trattamento dei dati personali dei lavoratori siano opportunamente protetti da indebite intrusioni. Inoltre, le comunicazioni personali riferibili esclusivamente a singoli lavoratori devono avvenire con modalità tali da escludere l'indebita presa di conoscenza da parte di terzi o di soggetti non designati quali addetti al trattamento dei dati personali dei dipendenti.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

12. LINEE GUIDA PER LA GESTIONE DEI SISTEMI INFORMATIVI

Utilizzo del computer aziendale

Il Personal Computer, sia fisso che portatile, affidato al dipendente è uno strumento aziendale di lavoro e non personale, pertanto vi devono essere archiviati dati relativi all'attività svolta e non dati propri. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

L'Amministratore di sistema, nei limiti delle incombenze e delle finalità affidate dalla Fondazione, gestisce e aggiorna il sistema informatico, attenendosi alle disposizioni del Titolare in tema di sicurezza. All'Amministratore di sistema è consentito l'accesso ai dati personali contenuti nelle banche dati esclusivamente e solo per il tempo necessario per garantire il buon funzionamento e la sicurezza del sistema informatico o per intervenire nel caso di perdita o violazione dei dati personali, secondo le disposizioni del Titolare. In applicazione del comunicato del Garante della Protezione dei dati personali del 14 gennaio 2008, il Titolare potrà adottare sistemi di controllo che consentono la registrazione degli accessi effettuati dagli Amministratori di sistema ai sistemi di elaborazione e agli archivi. La registrazione deve comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e saranno conservate per 1 anno.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione della Fondazione, perché sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore. Non è consentito utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici. La Fondazione si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.

Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente da Fondazione. Le violazioni della normativa a tutela del diritto di autore sul software sono sanzionate penalmente e l'inosservanza espone la Fondazione a gravi responsabilità. Non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine di scaricare materiale elettronico tutelato dalla normativa sul diritto di autore (software, file audio, film, etc).

Non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer, salvo previa autorizzazione della Fondazione. Le modifiche possono essere effettuate solo dall'Amministratore di sistema.

Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Per bloccare la schermata quando ci si assenta dalla postazione digitare il tasto Windows ⊞ + L .

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Non è consentita l'installazione sul proprio personal computer di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.), se non con l'autorizzazione della Fondazione. L'installazione è effettuata dall'Amministratore di sistema.

Al fine di garantire la disponibilità dei dati, anche e soprattutto in caso di violazioni, tutte le informazioni relative all'attività lavorativa vanno archiviate sugli applicativi autorizzati dalla Fondazione e non sul desktop del proprio computer.

Agli utenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account da più computer.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore del sistema e il Responsabile per la protezione dei dati personali nel caso in cui siano rilevati virus informatici ed adottando quanto previsto dai punti successivi del presente Regolamento aziendale e dalle norme del Regolamento che disciplinano la violazione dei dati.

Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

L'accesso ai PC aziendali in uso al dipendente è consentito alla Fondazione, attraverso l'Amministratore di Sistema, per ragioni tecniche e di sicurezza del sistema informatico. L'Amministratore di Sistema ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc... L'intervento viene effettuato su chiamata dell'utente o, in caso di oggettiva necessità, a seguito di rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non sia pregiudicata la tempestività e l'efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento

Una volta cessato il rapporto di lavoro, il PC aziendale va restituito alla Fondazione, la quale provvederà, attraverso l'Amministratore di Sistema, entro 30 giorni dalla cessazione del rapporto, a cancellare tutti i file non necessari e a salvare tutti i documenti aziendali necessari per assicurare la continuità lavorativa e la tutela della Fondazione.

Utilizzo della rete aziendale

Gli applicativi autorizzati dalla Fondazione sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, su questi applicativi. A tal fine, vengono svolte regolari attività di controllo da parte dell'Amministratore del sistema.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

L'Amministratore di sistema, informando la Fondazione e il Responsabile della protezione dei dati personali, può procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È da evitare un'archiviazione ridondante.

È cura dell'utente effettuare la stampa dei documenti aziendali, solo se strettamente necessaria. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio file di contenuto grafico) sulle multifunzioni. In caso di necessità la stampa in corso può essere cancellata.

A richiesta della Fondazione, ove si renda necessario al fine di tutelare i beni aziendali, oppure per eseguire accertamenti o interventi tecnici, l'Amministratore di sistema può estrarre un report delle stampe effettuate attraverso le stampanti multifunzioni e associate al codice identificativo del dipendente risultante dal badge personale.

Gestione delle password

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dall'Amministratore del sistema. È consentita l'autonoma sostituzione da parte degli incaricati al trattamento**.**

Le password devono avere un minimo di 8 caratteri e possono essere formate da lettere (maiuscole o minuscole) e numeri e simboli ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema. È obbligatorio realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi di cui sotto:

Caratteri minuscoli: a, b, c…

Caratteri maiuscoli: A, B, C…

Caratteri numerici: 0,1,2,3…

Caratteri non alfanumerici: !, /, ?, […

Le password utilizzate dagli incaricati al trattamento hanno una durata predeterminata dall'amministratore di sistema, trascorsi i quali le password devono essere sostituite. Non sarà possibile immettere una nuova password che sia identica alle ultime tre precedenti.

Le password vengono revocate alla cessazione del rapporto tra il dipendente e la Fondazione.

La password non deve essere comunicata a sconosciuti e deve essere immediatamente sostituita, nel caso si sospetti che la stessa abbia perso la segretezza, dandone comunicazione al Responsabile dell'Ufficio e al Responsabile della protezione dei dati personali.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile dell'Ufficio e al Responsabile della protezione dei dati personali.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Utilizzo dei supporti magnetici

L'utilizzo di supporti magnetici (pendrive, cd, dvd, etc) possono veicolare virus o programmi in grado di prendere il controllo del pc. Prima di utilizzare il supporto, è buona norma effettuare la scansione della periferica.

Tutti i supporti magnetici riutilizzabili (pen drive, cd, dvd) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.

Gli utenti in possesso di smart card/token per la firma digitale non devono abbandonarla devono rimuoverla dall'apposito alloggiamento nel caso di allontanamento del dipendente dalla postazione di lavoro. La smart card/token per a firma digitale deve essere custodita in contenitore chiuso a chiave.

Non è consentito scaricare files contenuti in supporti magnetici/ ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

Nel caso di files di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, è bene non aprirli, perché potrebbero contenere virus o programmi trojan horse capaci di prendere il controllo di pc o smartphone. In tal caso, va consultato previamente l'Amministratore di sistema.

Utilizzo di PC portatili, smartphone, tablet aziendali

L'utente è responsabile del PC portatile, dello smartphone, del tablet e di ogni altro strumento assegnatogli dalla Fondazione e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto.

L'utilizzo di pc portatili, smartphone, tablet o altri dispositivi personali all'interno dell'azienda, per finalità connesse all'attività lavorativa, è soggetto alle medesime regole del presente Regolamento. In ogni caso, la risorsa che intendesse fare uso di dispositivi personali all'interno dell'azienda per svolgere la propria attività lavorativa è tenuta a garantire medesimi standard di sicurezza informatica, o quanto meno equivalenti, a quelli adottati dalla Fondazione. L'utilizzo di dispositivi personali per attività lavorative deve essere autorizzato dalla Fondazione, dando senza ritardo comunicazione all'Amministratore di Sistema.

Uso della posta elettronica

La casella di posta, assegnata dalla Fondazione all'utente, è uno strumento di lavoro di proprietà della Fondazione e deve essere utilizzato soltanto per finalità aziendali. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Poiché le caselle sul dominio

"fondazionemaxxi.it" sono di proprietà della Fondazione, che ne concede l'uso ai dipendenti secondo le norme regolamentari in uso, gli utenti assegnatari sono responsabili del corretto utilizzo delle stesse.

La Fondazione protegge l'accesso agli account di posta elettronica attraverso MFA (MultiFactor Access) per garantire una maggiore sicurezza dei dati e delle informazioni raccolte. Accedendo all'account per la prima volta da un nuovo dispositivo o da una nuova applicazione, oltre al nome utente e alla password, sarà necessario un ulteriore fattore di autenticazione per confermare la propria identità. In questo modo, se un altro utente dovesse provare ad accedere, immettendo il nome e la password, ma senza specificare il secondo fattore, sarà bloccato. L'autenticazione a più fattori verrà usata la prima volta che si accede ad un dispositivo o ad una nuova applicazione, o dopo la modifica della password.

La Fondazione può inserire nei messaggi l'avvertimento ai destinatari che trattasi di un account di posta aziendale e che le risposte potranno essere conosciute dal personale di appartenenza della Fondazione.

E' fatto divieto di utilizzare le caselle di posta elettronica aziendale *……@fondazionemaxxi.it* per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list, salvo diversa ed esplicita autorizzazione della Fondazione; è consentito accedere alla casella di posta elettronica aziendale al di fuori della rete aziendale.

E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per la Fondazione, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere autorizzata dalla Fondazione. In ogni caso, è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La Fondazione mette a disposizione di ciascuno l'apposita funzione "fuori sede" che consente di inviare automaticamente, in caso di assenze, messaggi di risposta contenenti le coordinate (telefoniche o telematiche) di un altro soggetto o altre modalità di contatto dell'Ufficio. Le risorse della Fondazione sono tenute ad avvalersi di tali modalità per assicurare la continuità lavorativa, consentendo, ad esempio, l'apertura della posta elettronica da parte di persona espressamente autorizzata. In caso di assenza non programmate (ad esempio, malattie), qualora la risorsa non possa avviare la procedura di cui sopra, il titolare del trattamento, perdurando l'assenza oltre 2 giorni potrà disporre lecitamente, mediante l'amministratore di sistema, di attivare un accorgimento analogo, avvertendo gli interessati.

La stessa procedura deve essere attuata quando, per garantire l'ordinaria operatività aziendale, sia necessario accedere ad informazioni o documenti di lavoro presenti sul PC del dipendente assente.

I contenuti delle email aziendali vengono conservati per 5 anni e sino a 30 giorni dopo la cessazione del rapporto di lavoro. In ogni caso, è fatto obbligo al dipendente archiviare i documenti necessari per lo svolgimento dell'attività lavorativa, via via che giungono all'indirizzo email aziendale.

Le email aziendali aventi contenuto commerciale e a rilevanza giuridica vanno conservate per 10 anni per ottemperare agli obblighi legislativi in materia fiscale e civile. In ogni caso, è fatto obbligo al dipendente archiviare tali documenti via via che pervengono all'indirizzo email aziendali.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Alla data di cessazione del rapporto di lavoro, e comunque non oltre 48 ore dalla stessa, l'Ufficio per la gestione del personale informa l'Amministratore di sistema della cessazione del rapporto di lavoro: a partire da tale data, l'indirizzo email del dipendente sarà sospeso per 30 giorni, durante i quali sarà attiva una risposta automatica per reindirizzare gli interessati e comunicare agli stessi un recapito (telefonico o telematico) alternativo di destinazione, al fine di garantire la continuità lavorativa aziendale. Scaduto il termine di 30 giorni, i contenuti dell'account aziendale saranno cancellati.

In caso di esigenze tecniche e di sicurezza particolari, ovvero per rispondere ad un ordine dell'Autorità Giudiziaria o della polizia giudiziaria, ovvero, infine, ove vi sia l'evidenza o il fondato sospetto che il dipendente cessato abbia utilizzato a fini privati l'account aziendale o al fine di danneggiare l'azienda o beni aziendali, la Fondazione, attraverso persona specificatamente autorizzata e l'Amministratore di sistema, potrà accedere alle comunicazioni elettroniche in transito sull'account aziendale del dipendente cessato, al fine di tutelarsi, anche contro responsabilità o danni cui possa aver dato origine il comportamento del lavoratore. In queste ipotesi, la Fondazione potrà utilizzare le informazioni contenute nell'account aziendale e indispensabili per le finalità specificamente indicate.

E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, pec).

Per la trasmissione di file all'interno della Fondazione è possibile utilizzare gli applicativi messi a disposizione dalla Fondazione tramite l'interfaccia web; in alternativa la posta elettronica, prestando attenzione alla dimensione degli allegati.

E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

E' vietato inviare catene telematiche (o di "Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore del sistema. Non si deve in alcun caso attivare gli allegati di tali messaggi.

In considerazione di comportamenti anomali occorsi, e al fine di tutelare la sicurezza delle informazioni, vengono memorizzati i dati di log standard di sistema generati automaticamente per ciascuna email riguardanti: indirizzo email del mittente, indirizzo email del destinatario, indirizzo IP del server mittente, indirizzo IP del server destinatario, data ed ora, numero destinatari, dimensioni in byte del messaggio, tempo impiegato per la consegna, stato di consegna. La memorizzazione dei dati di log viene mantenuta per impostazione predefinita per 2 mesi. I termini di conservazione potranno essere prolungati per specifiche esigenze tecniche o di sicurezza, per ottemperare ad ordini dell'Autorità Giudiziaria o della polizia giudiziaria, per tutelare o esercitare un diritto in sede giudiziaria.

Uso della rete Internet e dei relativi servizi

I PC, gli smartphone, e ogni altro strumento abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa o in siti che accolgono contenuti contrari alla morale e alle prescrizioni di legge.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Museo nazionale delle arti del XXI secolo

Non è consentito navigare in siti che possano rivelare una profilazione dell'individuo relativa a dati particolari ai sensi del Regolamento UE n. 679/2016: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente e le sue abitudini sessuali.

E' fatto divieto all'utente scaricare software gratuiti (freeware) e shareware prelevati da siti Internet, se non espressamente autorizzato dalla Fondazione.

Le transazioni finanziarie ivi comprese le operazioni di remote banking, acquisti on-line e simili sono autorizzate dal Titolare, per le finalità della Fondazione, e con il rispetto delle normali procedure di acquisto.

E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

Non è consentito l'utilizzo di applicativi che nascondono la navigazione sul web.

Durante l'orario di lavoro, è vietata la partecipazione a forum non professionali e a giochi in rete pubblica l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

La Fondazione può regolare la connessione con un proxy che blocca l'accesso a siti web non autorizzati (come socialnetwork o siti che hanno contenuti contrati alla morale o alle autorizzazioni di legge).

Le attività sull'uso del servizio di accesso a internet sono automaticamente registrate in file di log, che riportano i dettagli della navigazione, i siti e i documenti consultati.

La conservazione dei dati personali relativi agli accessi ad internet e al traffico telematico avverrà per impostazione predefinita 1 mese e per ragioni di controllo del buon funzionamento e per la sicurezza del sistema informatico, nonché per esigenze organizzative e produttive. I tempi di conservazioni potranno essere prolungati (limitatamente alle solo informazioni indispensabili per perseguire finalità preventivamente determinate) in caso di esigenze tecniche o di sicurezza particolari, in caso di indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria, ovvero per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Nel caso di contenziosi o pre-contenziosi o per ottemperare ad una specifica richiesta dell'Autorità giudiziaria o della polizia giudiziaria o per adempiere ad un obbligo di legge, il Titolare del trattamento si riserva di conservare il dato se indispensabile per finalità descritta.

Il trattamento dei dati contenuti nei log può avvenire in forma anonima e/o aggregata (riferita alla singola struttura).

L'accesso al data base dei log è riservato all'Amministratore di Sistema, attraverso il pannello di controllo dei log di dominio oppure, per i log registrati sui computer aziendali, attraverso l'accesso diretto al computer, per rispondere ad eventuali richieste dell'autorità giudiziaria o della polizia giudiziaria, su richiesta del Segretario Generale qualora si verifichi un evento dannoso o di pericolo che richiede un immediato intervento o si verifichi un utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura, ovvero quando vi sia l'evidenza o il fondato sospetto che sia stato posto in essere un illecito. Anche l'accesso al data base da parte dell'Amministratore di sistema è oggetto di registrazione e i dati sono conservati per la durata di 6 mesi.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

Protezione antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Se si ricevono messaggi che avvisano di un nuovo virus pericolosissimo, vanno ignorati: le email di questo tipo sono dette hoax (bufale, leggende metropolitane). Questo è vero anche se il messaggio proviene da un contatto conosciuto, o da microsoft, ibm etc.. In ogni caso non vanno aperte email e/o relativi allegati sospetti.

Analogamente, tutti i messaggi che invitano a diffondere la notizia quanto più possibile sono hoax. Anche se parlano della fame del mondo o promettono guadagni miracolosi, sono tutti hoax che hanno lo scopo di utilizzare indebitamente le risorse informatiche. Contribuire alla loro diffusione può condurre all'esclusione del proprio accesso alla rete.

Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.

Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente: a) sospendere ogni elaborazione in corso senza spegnere il computer; b) segnalare l'accaduto all'Amministratore di sistema; c) informare il Responsabile della protezione dei dati personali.

Non è consentito l'utilizzo di cd rom, cd riscrivibili, nastri magnetici di provenienza ignota. In ogni caso, è bene verificare all'inserimento sul computer di memorie di massa rimovibili l'eventuale presenza di virus e malware con verifica manuale o automatica.

Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato all'amministratore di sistema.

Osservanza delle disposizioni in materia di Privacy

In ogni caso, è obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali adottate dalla Fondazione ovvero previste dalle norme di legge in materia.

Riservatezza nelle comunicazioni di informazioni

Anche le informazioni aziendali ritenute non riservate assumono diversa importanza e necessitano di analoga tutela, se comunicate a terzi. Occorre prestare molta attenzione a chi, presentandosi personalmente o contattandoci telefonicamente o mediante posta elettronica, inducendo fiducia o curiosità, richiede informazioni apparentemente innocue sulla Fondazione o la sua organizzazione e il personale che vi lavora ma possono raggiungere dati anche riservati.

Analogamente, occorre prestare attenzione a chi induce ad ottenere l'esecuzione di istruzioni contenute in un messaggio di posta elettronica: ad esempio, false comunicazioni email aventi forma, grafica e loghi di enti noti come assicurazioni, banche, posta, inps, che richiedono informazioni attraverso moduli o link a pagine web debitamente camuffate.

Non bisogna fornire informazioni confidenziali al telefono o di persona a interlocutori sconosciuti o aprire messaggi con allegati sospetti o da fonte sconosciuta; non utilizzare link contenuti nel testo del messaggio; non trasmettere informazioni in risposta a richieste provenienti da fonti istituzionali (banca, posta, inps, etc) in quanto tali soggetti non utilizzano queste modalità per chiedere informazioni. In casi dubbi, occorre contattare il Titolare o il Responsabile della protezione dei dati.

Controlli, monitoraggio e non osservanza della normativa aziendale

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

Il Titolare del trattamento può effettuare controlli sull'uso dei dispositivi elettronici, nel caso in cui si riscontri un utilizzo anomalo degli strumenti aziendali.

Nel rispetto dei principi di pertinenza e non eccedenza, il Titolare potrà effettuare preliminarmente, attraverso l'Amministratore di sistema, un controllo sui dati aggregati, riferiti all'intera struttura lavorativa o ad una sua area. All'esito del controllo anonimo, il Titolare può emanare un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. L'avviso può essere circoscritto ai dipendenti afferenti l'area o il settore in cui si è registrata l'anomalia. Nel caso in cui dovesse perdurare l'anomalia, il Titolare può effettuare un controllo su base individuale o su singole postazioni di lavoro, anche ex post.

Analogamente e con la medesima graduazione, la Fondazione può effettuare, attraverso l'Amministratore di sistema e/o altra persona espressamente autorizzata, controlli sulla posta elettronica aziendale messa a disposizione del dipendente, in base ad una motivazione specifica e a seguito di eventi effettivi che motivino, specificatamente, un intervento in tal senso.

L'accesso ai contenuti della casella elettronica del dipendente in servizio avviene attraverso l'Amministratore di sistema e/o altra persona autorizzata dalla Fondazione, previo avviso all'utente, salvo sussistano situazioni indifferibili e urgenti (tecniche e di sicurezza, ordine dell'Autorità Giudiziaria o della polizia giudiziaria, obbligo di legge, evidenza o fondato timore della commissione di un illecito), espressamente indicate, che giustificano un intervento immediato. Non appena possibile, e compatibilmente alle esigenze descritte, viene data comunicazione al dipendente.

Per finalità di assistenza, manutenzione e aggiornamento e previo tempestivo avviso all'utente, l'Amministratore di sistema potrà accedere da remoto al PC del dipendente attraverso un apposito programma software. I dati personali del dipendente potranno pertanto venire a conoscenza dell'Amministratore di sistema.

L'Amministratore di sistema effettuerà, inoltre, attività di monitoraggio e verifica delle protezioni predisposte sul sistema informativo rispetto ad aggressioni esterne, senza che siano necessarie preventive ulteriori informative. I risultasti del monitoraggio e della verifica potranno essere utilizzati soltanto in modo proporzionato e pertinente alle finalità e alla natura connesse.

FONDAZIONE MAXXI
Via G. Reni, 4A – 00196 Roma
t. 063201954
e. privacy@fondazionemaxxi.it
c.f. 10587971002

DISPOSIZIONI FINALI

Per quanto non previsto nel presente Regolamento, si applicano le disposizioni del Regolamento (UE) n. 2016/679, come recepito nell'Ordinamento Italiano, nonché i provvedimenti del Garante per la protezione dei dati personali.

Il presente Regolamento potrà essere modificato e integrato in base a sopraggiunte variazione della normativa nazionale e transnazionale applicabile e sulla base di documentate esigenze organizzative e funzionali.

***

Aggiornato nel maggio 2023