SISTEMA SANITARIO REGIONALE
AZIENDA OSPEDALIERO-UNIVERSITARIA
SANT'ANDREA

REGIONE LAZIO

SAPIENZA
UNIVERSITÀ DI ROMA

PROCEDURA
DATA BREACH

Versione 1

Scheda descrittiva

Anagrafica del documento

Titolo	**:**	Procedura data breach
Tipo documento	**:**	Procedura
Descrizione	**:**	Il documento descrive le modalità operative da seguire in caso di violazione dei dati personali avvenuta sia a seguito di trattamento informatizzato sia a seguito di trattamento cartaceo.

Dati identificativi

Vers	Note di revisione	Data di emissione	Elaborato	Verificato	Approvato
1	Prima emissione	25/05/2018	LEGALE + ICT	Responsabile della protezione dei dati	Titolare del trattamento nella persona dell'AD

INDICE

1 PREMESSA

Il 25 maggio 2018 entra in vigore in tutti i Paesi europei il Regolamento generale sulla protezione dei dati 2016/679 (di seguito “GDPR”) con ricadute organizzative, operative e tecnologiche che riguardano i principali processi di gestione dei dati personali. Tra le novità contenute nel Regolamento, anche alcuni oneri aggiuntivi per la gestione degli incidenti di sicurezza che comportano la violazione di dati personali (data breach).

Il presente documento descrivere i criteri per individuare una violazione di dati personali e per valutare i casi in cui la violazione debba essere notificata all’Autorità di controllo e agli interessati, in conformità con le indicazioni del GDPR.

Nel paragrafo 5 sono presi in considerazione gli eventi relativi a trattamenti informatizzati nel caso in cui la eventuale violazione avvenga nell’ambito dei servizi ICT e delle applicazioni gestiti dalla Società

Infine nel paragrafo 6 sono trattati gli eventi relativi a trattamenti non informatizzati.

2 CONTESTO DI RIFERIMENTO E QUADRO GIURIDICO

Le norme di riferimento sono:

1. Regolamento UE n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);
2. Documento WP 250 “Guidelines on Personal data breach notification under Regulation 2016/679” del 3 ottobre 2017.

3 CRITERI PER INDIVIDUARE E CLASSIFICARE UN DATA BREACH

Un data breach, o violazione di dati personali, è un incidente 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”.*

In relazione ad un evento che si è verificato o che si presume si possa verificare (minaccia) come conseguenza di un altro evento illecito o accidentale, la violazione di dati personali viene classificata in tre tipologie:

Tipologia di violazione	Evento/Minaccia
Violazione di riservatezza	Accesso o trattamento non autorizzato o illecito
	Divulgazione non autorizzata
Violazione di integrità	Modifica non autorizzata o accidentale
Violazione di disponibilità	Perdita o distruzione accidentale o illegale
	Indisponibilità temporanea o prolungata

Tabella 1 – Classificazione di un data breach

Le tipologie non sono mutuamente esclusive: una violazione di dati personali può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità, una di esse o una loro combinazione.

4 NOTIFICHE E COMUNICAZIONI

Il GDPR prevede che il Titolare del trattamento debba notificare la violazione di dati personali all'Autorità di controllo e agli interessati se questa comporta dei rischi per i diritti e le libertà delle persone fisiche coinvolte.

In presenza di un data breach, quindi, il Titolare stima tale rischio e decide, sulla base del risultato ottenuto e delle circostanze in cui l'evento si è verificato, se procedere alle relative notifiche.

I prossimi paragrafi riportano:

- le modalità di valutazione del rischio per i diritti e le libertà degli interessati in caso di violazione di dati personali;
- i criteri che fanno scattare l'obbligo di notifica all'Autorità di controllo e le modalità di notifica;
- i criteri che fanno scattare l'obbligo di comunicazione agli interessati e le modalità di notifica.

4.1 VALUTAZIONE DEL RISCHIO PER I DIRITTI E LE LIBERTÀ DELL'INTERESSATO

Nel seguito viene illustrata la metodologia adottata per la valutazione del rischio per i diritti e le libertà dell'interessato derivante da un trattamento di dati personali che avvenga sia mediante strumenti informatici e telematici, sia manuali.

Il rischio per l'interessato, che può assumere i valori Medio (M) o Alto (A), viene valutato sulla categoria dei dati personali trattati (cfr. Appendice 2) in base alla gravità del danno (fisico-biologico, finanziario, reputazionale e di identità) e alla probabilità di accadimento delle minacce riportate in tabella 1.

Minaccia	Categoria di dati personali	Rischio per l'interessato
Accesso, trattamento non autorizzato o illecito	Dati personali comuni	M
	Dati sensibili	A
	Dati ipersensibili	A
	Dati specifici	A
	Dati giudiziari	A
	Dati biometrici	A
	Dati personali comuni	M
	Dati sensibili	A

Minaccia	Categoria di dati personali	Rischio per l'interessato
Divulgazione non autorizzata o accidentale	Dati ipersensibili	A
	Dati specifici	A
	Dati giudiziari	A
	Dati biometrici	A
Modifica non autorizzata o accidentale	Dati personali comuni	M
	Dati sensibili	A
	Dati ipersensibili	A
	Dati specifici	A
	Dati giudiziari	A
	Dati biometrici	A
Perdita, distruzione accidentale o illecita	Dati personali comuni	M
	Dati sensibili	A
	Dati ipersensibili	A
	Dati specifici	A
	Dati giudiziari	A
	Dati biometrici	A
Indisponibilità temporanea o prolungata	Dati personali comuni	M
	Dati sensibili	A
	Dati ipersensibili	A
	Dati specifici	A
	Dati giudiziari	A
	Dati biometrici	A

Tabella 2 - Valori di rischio per i diritti e le libertà dell"interessato

Una volta individuato e classificato un data breach come descritto nel paragrafo 3, vengono considerati i valori di rischio corrispondenti agli eventi che si sono verificati o che si presume si possano verificare in seguito all'incidente.

Come si desume dalla tabella, il rischio per l'interessato è Medio solo nel caso in cui i dati trattati appartengano alla categoria "dati personali comuni" (cfr. Appendice 2).

Il rischio per l'interessato può essere aumentato in considerazione dei seguenti fattori (cfr. Documento WP 250 "Guidelines on Personal data breach notification under Regulation 2016/679" del 3 ottobre 2017):

- la natura, la sensibilità e il volume dei dati violati. Una violazione di più dati personali riferiti alla stessa persona, infatti, può aumentare la gravità del danno per l'interessato;
- la facilità di identificare specifici individui;
- l'analisi del contesto in cui si è verificata la violazione (attacco informatico, errore umano, …);
- le caratteristiche specifiche degli interessati (minori, categorie vulnerabili, …);

- la numerosità degli interessati, qualora indica sulla gravità del danno.

4.2 NOTIFICA ALL'AUTORITÀ DI CONTROLLO IN CASO DI INDISPONIBILITÀ DEI DATI PERSONALI

Il GDPR prevede che il Titolare del trattamento debba notificare all'Autorità di controllo una violazione di dati personali *"senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche".*

Per quanto riguarda il caso particolare della indisponibilità temporanea o prolungata di dati personali dovuta ad indisponibilità del servizio che li tratta (ad esempio nel caso di attacchi di tipo *denial of service* o di assenza di connettività Internet), tra i fattori di valutazione deve essere incluso il tempo in cui i dati non sono disponibili. Se viene garantita la continuità operativa o il ripristino in tempi adeguati per scongiurare un danno per gli interessati, la notifica all'Autorità di controllo non è necessaria.

Per decidere di procedere alla notifica si adotta la seguente tabella:

	Rischio totale per l'interessato	
Durata indisponibilità del servizio	**Alto**	**Medio**
Minore di 1 ora	Nessuna notifica	Nessuna notifica
Da 1 ora a 4 ore	Notifica	Nessuna notifica
Oltre 4 ore	Notifica	Notifica

Tabella 3 - Notifica all'Autorità di controllo in base ai tempi di indisponibilità del servizio

Nel caso in cui la violazione non riguardi solo l'indisponibilità, ma anche altri eventi certi o presunti (ad esempio si suppone che i dati, oltre a essere indisponibili, siano stati acceduti illecitamente), la valutazione, pur tenendo conto dei tempi di indisponibilità indicati in tabella, deve comprendere l'analisi di tutti gli eventi correlati.

4.3 COMUNICAZIONE AGLI INTERESSATI

Quando il rischio per l'interessato, valutato come specificato nel paragrafo 4.1, assume il valore Alto ("rischio elevato", GDPR art. 34), la violazione deve essere comunicata anche agli interessati.

Fanno eccezione i seguenti casi:

- i dati violati sono stati preventivamente protetti da misure tecniche e organizzative adeguate a scongiurare un rischio elevato per gli interessati (ad esempio la cifratura o la pseudonimizzazione);
- dopo la violazione sono state adottate misure che abbassano almeno a Medio il rischio totale per l'interessato;

- i dati personali sono stati indisponibili per un periodo di tempo inferiore a 1 ora e non si è verificata alcuna altra tipologia di violazione;
- la comunicazione richiede un impegno spropositato. È il caso, ad esempio, di violazioni massive di dati. In queste circostanze si può procedere a una comunicazione pubblica o di pari efficacia.

La comunicazione deve descrivere, in linguaggio semplice e chiaro, la natura della violazione e deve inoltre contenere:

- il nome e i dati di contatto del Responsabile della protezione dei dati, del Titolare del trattamento o di altro contatto da cui ottenere maggiori informazioni;
- la descrizione delle probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e attenuarne i possibili effetti negativi.

5 TRATTAMENTI INFORMATIZZATI

Per trattamenti informatizzati nell'ambito di questo documento si intendono quelli effettuati mediante applicazioni o strumenti di office automation.

Nell'ambito dell'operatività interna nel caso in cui si verifichino uno o più eventi di cui alla Tabella 1, il flusso operativo che viene seguito è di seguito illustrato:

1. l'Ufficio ICT nel corso della gestione di un evento rileva una possibile "violazione di dati personali" (Data Breach) e ne dà immediata notifica al Titolare e al DPO. Provvede, quindi, alla compilazione del rapporto d'incidente (Appendice 3 – rapporto di incidente).

2. L'Ufficio ICT svolge le attività di verifica, eventualmente con il supporto di Core Sistemi S.r.l. e UNO Informatica S.r.l.

3. In caso di esito negativo della valutazione, l'Ufficio ICT termina il processo, notificando al Titolare e al DPO della Società l'identificativo dell'incidente chiuso e le motivazioni, completando con la chiusura il relativo rapporto di incidente.

4. In caso, invece, di esito positivo l'Ufficio ICT completa la compilazione del rapporto di incidente già aperto proponendo una valutazione di impatto e gravità del rischio per i diritti e le libertà delle persone fisiche e lo trasmette immediatamente al Titolare e al DPO.

5. Il Titolare, di concerto con il DPO, valuta il livello di gravità della "violazione di dati personali" proposto dall'Ufficio ICT e lo accetta oppure lo modifica.

Nel caso in cui la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare, di concerto con il DPO, provvede a inoltrare la notifica con tutte le informazioni di cui al paragrafo 4.3 all'Autorità di Controllo entro 72 ore dalla conoscenza dell'avvenuta compromissione dei dati personali. Qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

E' possibile che si verifichino anche eventi di cui alla Tabella 1 nel caso, residuale, in cui dati personali siano trattati non nell'ambito di servizi ICT ma su postazioni di lavoro fisse o portatili.

Di seguito si elencano le più frequenti circostanze che possono condurre alla violazione di dati:

1) Mancato rispetto delle regole comportamentali contenute nella sezione “Regolamento per l’utilizzo della rete informatica aziendale” contenuta nel Regolamento interno;

2) Furto o smarrimento dispositivi portatili;

3) Rottura accidentale di componenti (hard disk) di PC fissi o portatili.

Il rischio che si verifichi la circostanza di cui al punto 2 è mitigato da misure di sicurezza quali cifratura dati e backup di apposite directory in cloud, in cui gli utenti conservano i dati di maggior rilevanza, e formattazione remota per i cellulari.

Con riferimento alla minaccia di cui al punto 3, le misure di sicurezza adottate sono il backup di apposite directory in cloud per i dispositivi portatili e l’utilizzo di cartelle di rete, su cui sono definite opportune policy di backup.

5.1 FORM DI NOTIFICA

La comunicazione all’Autorità di Controllo deve contenere necessariamente i seguenti dati:

- tipologia di incidente;
- descrizione del servizio impattato e/o della banca/banche dati oggetto di violazione di dati personali;
- intervallo temporale dell’incidente;
- luogo dell’incidente;
- misure tecniche di sicurezza applicate ai dati violati;
- misure attivate per il contenimento e la prevenzione;
- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- descrizione della probabile conseguenza della violazione dei dati personali;
- descrizione delle misure di sicurezza adottate o di cui si propone l’adozione da parte del Titolare del trattamento per porre rimedio alla violazione di dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- proposta di comunicazione di violazione di dati personali all’/agli interessato/i in base ad un’analisi dei dati oggetto di violazione (qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche) e non ricorrendo alcuna delle condizioni di cui all’articolo 34, comma 3, del GDPR, che escludono la necessità di comunicazione della violazione all’interessato;
- il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- i dati organizzativi di riferimento e i relativi recapiti della Società;
- il livello di gravità della violazione;
- l’eventuale comunicazione agli interessati e le relative modalità;
- qualora la notifica all’Autorità di Controllo non sia effettuata entro 72 ore, i motivi del ritardo.

6 TRATTAMENTI NON INFORMATIZZATI

Per trattamenti non informatizzati nell'ambito di questo documento si intendono quelli effettuati senza l'ausilio di strumenti elettronici, ovvero nei casi in cui i dati risiedono su supporto cartaceo.

Anche per questa tipologia di trattamento si fa riferimento alla metodologia adottata per la valutazione del rischio per i diritti e le liberà dell'interessato illustrata nel paragrafo 4.1.

In tale ambito assumono significativa rilevanza le istruzioni impartite per iscritto, sia al momento della nomina sia mediante apposite policy aziendali, alle persone autorizzate (c.d. Incaricati) finalizzate all'utilizzo, al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali, in special modo se contenenti dati personali sensibili o giudiziari, e l'adozione degli adeguati comportamenti da parte degli incaricati stessi.

In particolare il Titolare:

- individua, e verifica periodicamente, gli incaricati del trattamento che utilizzano strumenti non automatizzati per la raccolta e la gestione di dati personali e impartisce loro istruzioni scritte relative alla gestione dei dati e alla loro custodia;
- identifica e comunica agli incaricati gli archivi in cui riporre i documenti contenenti i dati personali e/o categorie particolari di dati (armadi chiusi a chiave, stanze chiuse a chiave, casseforti di sicurezza, ecc.);
- istruisce le persone autorizzate affinché i documenti cartacei vengano conservati in archivi adeguatamente protetti per evitare la lettura e/o il prelievo non autorizzato, garantendo, quindi, la riservatezza e l'integrità dei dati personali in essi contenuti;
- dispone che i documenti cartacei vengano custoditi in appositi archivi chiusi a chiave, in armadi o stanze, al termine della giornata lavorativa; le chiavi devono essere risposte in un luogo sicuro e non lasciate nelle serrature stesse;
- prevede, ove possibile, la conservazione dei documenti contenenti dati personali di categorie particolari (ad esempio sensibili e/o giudiziari) separata dai documenti contenenti dati personali comuni;
- dispone che il trattamento di dati personali e/o di categorie particolari degli stessi avvenga nel rispetto del principio di limitazione della finalità, ovvero unicamente per lo scopo per cui sono stati raccolti;
- istruisce le persone autorizzate affinché:
  - i dati personali e/o le categorie particolari degli stessi non vengano diffusi o comunicati a soggetti non autorizzati al trattamento;
  - non vengano lasciati incustoditi documenti contenenti i dati personali e/o le categorie particolari degli stessi durante e dopo l'orario di lavoro;
  - non vengano lasciati in luoghi accessibili al pubblico i documenti contenenti i dati personali e/o le categorie particolari degli stessi;
  - i documenti vengano riposti negli archivi quando non più operativamente necessari;
  - limitino allo stretto necessario l'effettuazione di copie dei suddetti documenti;

- verifichino la corretta esecuzione delle procedure di distruzione dei documenti, quando non più necessari o quando richiesto dall'interessato, attraverso l'utilizzo di opportuni strumenti (distruggidocumenti), in modo da rendere impossibile la ricostruzione del documento.

Nel caso in cui, nonostante tali misure adottate dal Titolare, si verifichino uno o più eventi di cui alla tabella 1, il flusso operativo che viene seguito è di seguito illustrato:

1. il Responsabile di ciascuna area, desumibile dall'organigramma adottato dalla Società, informato dall'incaricato della possibile "violazione di dati personali" (data breach), ne dà immediata comunicazione al Titolare e al Responsabile della protezione dei dati. Provvede, quindi, alla compilazione del rapporto d'incidente (Appendice 3 – Rapporto di incidente). Previo accordo con il Responsabile dell'area di appartenenza, può essere lo stesso incaricato a segnalare, senza ingiustificato ritardo, al Titolare o al Responsabile della Protezione dei dati qualsiasi ipotesi di violazione di sicurezza, provvedendo alla compilazione del rapporto d'incidente.
2. Il Responsabile della protezione dei dati svolge le attività di verifica.
3. In caso di esito negativo della valutazione, il Responsabile della protezione dei dati termina il processo, notificando al Titolare l'identificativo dell'incidente chiuso e le relative motivazioni, completando con la chiusura il relativo rapporto di incidente.
4. In caso, invece, di esito positivo, Responsabile della protezione dei dati completa la compilazione del rapporto di incidente già aperto proponendo una valutazione di impatto e gravità del rischio per i diritti e le libertà delle persone fisiche e lo trasmette immediatamente al Titolare.
5. Il Titolare, di concerto con il Responsabile della protezione dei dati, valuta il livello di gravità della "violazione di dati personali" proposto e lo accetta oppure lo modifica.

   Nel caso in cui la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare, di concerto con il Responsabile della protezione dei dati, provvede a inoltrare la notifica con tutte le informazioni di cui al paragrafo 5.1 all'Autorità di Controllo entro 72 ore dalla conoscenza dell'avvenuta compromissione dei dati personali. Qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Quando il rischio per l'interessato, valutato come specificato nel paragrafo 4.1, assume il valore Alto ("rischio elevato", GDPR art. 34), la violazione deve essere comunicata anche agli interessati secondo le modalità previste al paragrafo 4.3.

Appendice 1 – Acronimi e Glossario

Autorità di controllo (o autorità Garante)	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR.
Data breach (o violazione di dati personali)	"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" (GDPR, art. 4 punto 12).
Dato personale	"Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (GDPR, art. 4 punto 1).
Danno	Conseguenza negativa derivante dal verificarsi di una determinata minaccia; il danno può qualificarsi come materiale quando determina una concreta lesione all'ambito fisico o patrimoniale dell'interessato oppure immateriale quando riguarda le possibili conseguenze dannose derivanti dal trattamento di dati personali, di natura non patrimoniale e che affliggono la sfera interiore del soggetto interessato.
Responsabile della protezione dei dati	Soggetto cui è attribuito dal Titolare del trattamento il compito di informare e fornire consulenza sugli obblighi derivanti dal GDPR e di sorvegliarne l'osservanza. Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (PIA) e ne sorveglia lo svolgimento. Coopera con l'Autorità di controllo e funge da punto di contatto con essa (GDPR, art. 37, 38, 39).
GDPR	Regolamento Ue n. 679/2016 "*General Data Protection Regulation",* in italiano indicato come "Regolamento generale sulla protezione dei dati".
Interessato	La persona fisica cui si riferiscono i dati personali.
Minaccia	Una serie di eventi dannosi che possono compromettere le caratteristiche di integrità, riservatezza e disponibilità del dato personale.
Misura di sicurezza	Accorgimento tecnico e organizzativo utilizzato per garantire che i dati non vadano distrutti o persi anche in modo accidentale, per garantire che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.

Privacy Impact Assessment (PIA)	Valutazione d'impatto che deve essere compiuta dal titolare quando "un tipo di trattamento (…) può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (GDPR, art. 35).
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica o altro organismo che tratta dati personali per conto del titolare del trattamento.
Servizio ICT	Insieme di funzionalità informatiche omogenee destinate a supportare un processo o un'attività lavorativa. Un servizio informatico è composto da una o più applicazioni software e dalla relativa infrastruttura tecnologica di supporto.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Trattamento	Operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali, come la raccolta, la registrazione, la conservazione, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione, la distruzione, ecc.

Appendice 2 – Categorie di dati personali

Dati personali comuni	
Anagrafici	Dati personali anagrafici quali nome, cognome, data e luogo di nascita, stato civile, residenza.
Contabili, fiscali, inerenti possidenze e riscossione	Dati personali quali versioni parziali/integrali di documenti contabili, dati di dettaglio risultanti dalle dichiarazioni fiscali oppure dai cedolini dello stipendio di ciascun lavoratore, indicazioni di dati riferiti a percettori di somme (e.g. i recapiti individuali e le coordinate bancarie utilizzate per effettuare i pagamenti), complesso dei beni posseduti (e.g case, terreni, altre proprietà).
Inerenti il rapporto di lavoro	Dati personali inerenti l'esecuzione del rapporto di lavoro: tipologia di contratto e livello contrattuale, dettagli di assunzione, irrogazione di sanzioni disciplinari, stipendio, trasferimenti del lavoratore, etc.
Tracciamenti	Dati personali presenti nei tracciati record generati dalla registrazione delle operazioni svolte su sistemi, applicativi, ecc.
Dati inerenti situazioni giudiziarie civili, amministrative, tributarie	Trattamento di dati personali quali cartelle tributarie, pagamenti, rateizzazioni, procedure in corso, assenza o esistenza di condanne emesse, contenziosi pendenti.
Dati personali (comuni) specifici	
Dati che consentono geolocalizzazione	Dati personali derivanti dalla rilevazione di coordinate satellitari relative alla geolocalizzazione di apparati elettronici di tipo radio mobili e veicolari, celle territoriali agganciate dai ricevitori GPS, dati relativi agli indirizzi IP.
Audio/video/foto	Audio, video, fotogrammi, immagini che possano far riconoscere, tramite riconoscimento facciale, vocale e/o comportamentale, la persona fisica.
Dati di profilazione	Dati riguardanti aspetti personali relativi a una persona fisica, che ne consentano di identificare preferenze, interessi, analizzare o prevedere il rendimento professionale, la situazione economica, la salute, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti del soggetto.
Dati personali finanziari	
Dati relativi all'esistenza di rapporti finanziari (coordinate bancarie, consistenze saldi, movimenti, giacenza media, etc.)	Dati relativi alla situazione bancaria attuale e/o passata dell'interessato, informazioni gestite da operatori finanziari quali: i saldi iniziali e finali del rapporto, il totale dei movimenti annuali in entrata e in uscita, la c.d. giacenza annuale media etc.

Dati personali sensibili	
Convinzioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	Dati personali che possano rivelare convinzioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.
Dati personali ipersensibili	
Stato di salute, assistenza sanitaria, orientamento/vita sessuale	Sottoinsieme di dati sensibili attinenti: - lo stato di salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, dati idonei a rivelare informazioni relative al suo stato di salute, ad esempio, certificato medico, cartella clinica, etc. - l'orientamento sessuale e/o la vita sessuale della persona fisica
Genetici	Dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione.
Dati personali biometrici	
Impronte digitali	Dati personali relativi ad impronte digitali e caratteristiche della topografia della mano, utilizzate per l'identificazione degli esseri umani.
Altre caratteristiche biometriche	Dati relativi ad altre caratteristiche fisiche quali: retina, vascolarizzazione, forma del volto. Possono intendersi caratteristiche biometriche anche caratteristiche comportamentali quali impronta vocale, movimenti del corpo, stile di battitura sulla tastiera.
Firma grafometrica	Firma grafometrica, analoga alla firma “olografa”, inserita in un'apposita tavoletta elettronica con l'ausilio di una penna elettronica.
Dati personali giudiziari	
Casellario giudiziale	Dati contenuti all'interno del certificato penale del casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione).
Qualità di indagato/imputato o altre situazioni giudiziarie e reati o connesse misure di sicurezza	Dati idonei a rivelare che un determinato soggetto è stato sottoposto ad indagini di polizia giudiziaria, al termine delle quali, è stato accusato di un reato nell'ambito di un Procedimento penale (certificato dei carichi pendenti).

Appendice 3 – Rapporto di incidente

Incidente				
identificativo		data	ora	stato
Descrizione del contesto di presentazione dell'incidente				
Descrizione dell'incidente				
Componente applicativa				
nome			release	versione	Fornitore
funzionalità	tipologia oggetto d'interfaccia		identificativo oggetto d'interfaccia		
Componente hardware				
nome			numero di serie	Fornitore
funzionalità	tipologia oggetto		identificativo oggetto	
Descrizione della violazione dei dati a seguito di trattamento non informatico				
Dati raccolti nella fase di analisi				
Utilizzatore/i del sistema/applicazione/servizio				
Nominativo di chi ha rilevato l'incidente				
Nome	cognome	data e ora		
Nominativo di chi ha preso in carico l'incidente				
nome	cognome	data e ora		
Azione/i svolte				
Tipologia di dati coinvolti nell'incidente				
Valutazione del rischio per l'interessato a cura LEGALE-ICT				
Valutazione del rischio per l'interessato a cura Titolare e Responsabile della protezione dei dati				
Chiusura				
motivazione	data	ora		
