REGOLAMENTO AsFO
PER LA GESTIONE DEI *DATA BREACH*

Indice

CAPO I – DEFINIZIONI E OGGETTO DEL REGOLAMENTO

Articolo 1 – Definizioni (rilevanti per il presente Regolamento)

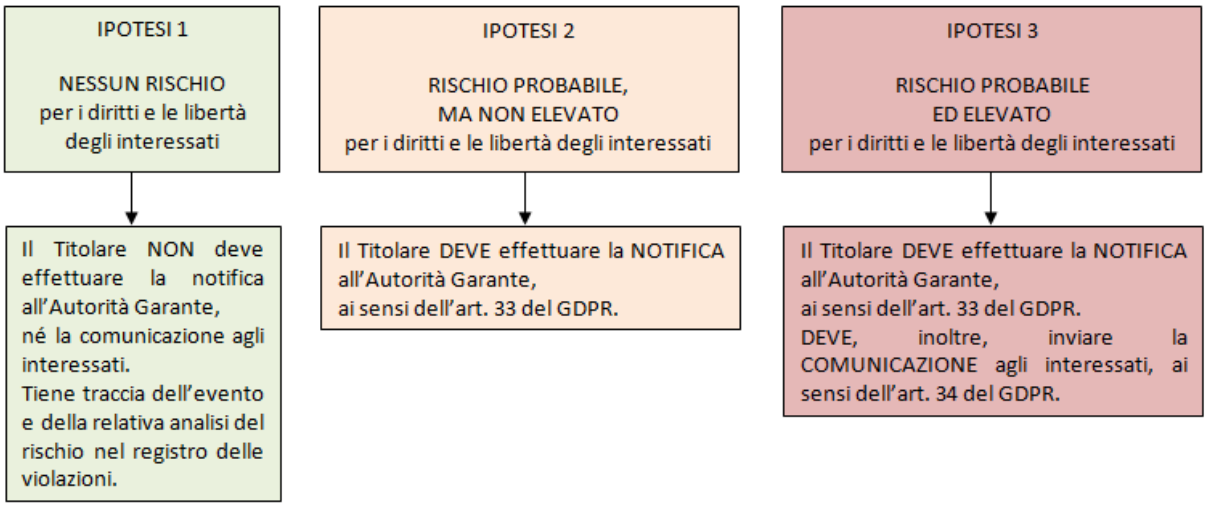
1. Ai fini del presente Regolamento si intende per:
   - **«GDPR»**: *General Data Protection Regulation*, ossia il Regolamento (UE) n. 2016/679 sulla protezione dei dati personali;
   - **«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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;
   - **«dato anonimo»**: il dato che in origine, o a seguito di trattamento, non può essere in alcun modo associato a un interessato identificato o identificabile;
   - **«trattamento di dati personali»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi 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;
   - **«Titolare del trattamento»**: 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; nel nostro caso, il Titolare è l'AsFO, rappresentata dal Direttore Generale *pro tempore*;
   - **«Delegati del trattamento»:** persone fisiche, che operano sotto l'autorità del Titolare, alle quali siano attribuiti dal Titolare medesimo, sotto la responsabilità e nell'ambito dell'assetto organizzativo dello stesso, specifici compiti e funzioni connessi al trattamento di dati personali;
   - **«Responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
   - **«Autorizzati al trattamento»**: persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare, dai Delegati o dai Responsabili del trattamento;
   - **«DPO»**: *Data Protection Officer*;
   - **«Autorità Garante per la Protezione dei Dati Personali»**: l'autorità pubblica indipendente deputata, nel nostro ordinamento, al controllo del rispetto della normativa vigente in materia di protezione dei dati personali;
   - **«Interessato»**: persona fisica cui si riferiscono i dati personali;
   - **«terzo»**: 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;
   - **«destinatario»**: 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;

- **«comunicazione»**: il dare conoscenza – in qualunque forma, anche mediante la messa a disposizione o consultazione – dei dati personali a uno o più soggetti determinati, diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli autorizzati;
- **«consenso dell'Interessato»**: 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;
- **«violazione dei dati personali» (*data breach*)**: 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.

Articolo 2 – Oggetto, finalità e ambito di applicazione del Regolamento

1. Il presente Regolamento – rivolto a tutto il personale che opera a qualsiasi titolo e a qualsiasi livello, direttamente o per conto di AsFO, su trattamenti di dati di titolarità AsFO – disciplina, in osservanza dei principi normativamente previsti in materia di *data protection* e tenendo conto della realizzabilità tecnica e della sostenibilità organizzativa aziendale:
    - le modalità di segnalazione al Titolare di una violazione di dati, anche potenziale;
    - il metodo di valutazione dell'evento accaduto;
    - le modalità di notifica obbligatoria – ove prevista – all'Autorità Garante per la Protezione dei Dati Personali;
    - le modalità per la comunicazione – ove prevista – agli Interessati.
2. Il presente Regolamento, nel costante rispetto del principio di *accountability* e a garanzia di un'efficace risposta aziendale ai fatti di *data breach*, è finalizzato a definire e a fornire una procedura aziendale di gestione delle eventuali violazioni di dati personali, chiarendone i passaggi essenziali, i soggetti a vario titolo coinvolti, i criteri di valutazione degli eventi.
3. Ciascun evento di *data breach* è annotato in apposito registro, il c.d. registro delle violazioni, allegato al presente Regolamento (Allegato 2).
4. La procedura regolata nel presente atto può essere graficamente rappresentata come segue:



CAPO II – TIPOLOGIE E OGGETTO DI *DATA BREACH*

Articolo 3 – Tipologie di violazioni dei dati

1. Le violazioni, come definite all'art. 1 del presente Regolamento, senza pretesa di esaustività, possono tradursi in:
   - distruzione → i dati non esistono più o non esistono più in una forma che sia di qualche utilità per l'Azienda, in quanto danneggiati o corrotti;
   - perdita definitiva → i dati potrebbero comunque esistere, ma l'Azienda potrebbe averne perso il controllo, l'accesso o il possesso. Qualora i dati non siano più recuperabili, la perdita è definitiva ed equivale a una distruzione. Un esempio di perdita definitiva può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un *ransomware*. Si ha perdita dei dati anche nel caso in cui l'Azienda abbia adottato come misura di sicurezza la crittografazione dei dati mediante una chiave non più in suo possesso;
   - perdita non definitiva → i dati non sono più nel possesso dell'Azienda, ma l'accesso agli stessi o il loro controllo può essere recuperato. Un esempio di perdita di dati personali può essere il furto di un dispositivo contenente una copia della banca dati in cui sono contenute informazioni personali degli Interessati. Un altro esempio può essere la cancellazione accidentale dei dati comunque conservati in copia. Può verificarsi, inoltre, perdita di disponibilità anche in caso di interruzione della fornitura di elettricità, che rende i dati personali temporaneamente non accessibili;
   - accesso non autorizzato → accesso al sistema dei dati personali da parte di un soggetto non autorizzato. Ciò comporta la visualizzazione non consentita dei dati, con l'ulteriore rischio di un'indebita appropriazione degli stessi da parte del terzo non autorizzato;
   - modifica non autorizzata → modifica dei dati personali, diversa dalla cancellazione, eseguita da un soggetto che non sia autorizzato a compiere tale operazione. La modifica illecita può derivare tanto da un accesso completamente illegittimo, quanto dall'accesso di un soggetto autorizzato alla modifica di una parte del *database*, il quale, però – in mancanza di adeguate misure di sicurezza – modifica dati di cui non dovrebbe avere la disponibilità;

- divulgazione non autorizzata → trasmissione dei dati personali, da parte di un soggetto non autorizzato, verso soggetti terzi oppure divulgazione di dati personali, da parte di un soggetto autorizzato, a terzi non abilitati alla ricezione degli stessi.

2. Le potenziali violazioni di dati personali così descritte si distinguono in:
   - violazioni informatiche → derivano da eventi che interessano applicativi o dispositivi informatici (ad esempio attacchi *hacker*, cancellazione di *database*, accessi abusivi alle reti aziendali, furto o diffusione illecita dei dati durante la trasmissione fra *software*, ecc.);
   - violazioni analogiche → derivano da eventi che non interessano applicativi o dispositivi informatici (ad esempio, smarrimento di documenti, distruzione di archivi cartacei, perdita di dispositivi rimovibili di archiviazione, ecc.).

Articolo 4 – Oggetto delle violazioni dei dati

1. Le violazioni di dati personali possono avere a oggetto:
   - la riservatezza → divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;
   - l'integrità → modifica non autorizzata o accidentale dei dati personali;
   - la disponibilità → perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

CAPO III – SEGNALAZIONE DI UN *DATA BREACH*

Articolo 5 – Segnalazione *data breach* da parte dell'Interessato

1. L'Interessato, o chi ne fa le veci, ha la facoltà di segnalare le potenziali violazioni dei dati personali che lo riguardano in una delle seguenti modalità:
   - trasmissione del modulo allegato al presente Regolamento (Allegato 3), corredato di fotocopia di un documento di identità in corso di validità, all'indirizzo *e-mail* privacy@asfo.sanita.fvg.it ovvero all'indirizzo di posta elettronica certificata (PEC) asfo.protgen@certsanita.fvg.it;
   - consegna *brevi manu* all'Ufficio Protocollo o all'Ufficio Privacy del modulo stesso, corredato di fotocopia di un documento di identità in corso di validità.

Articolo 6 – Segnalazione *data breach* interni alla struttura

1. I Delegati e gli Autorizzati al trattamento ai sensi del Regolamento aziendale per la protezione dei dati personali (rif. Decreto del Direttore Generale n. 723 del 26 novembre 2020) sono tenuti a segnalare tempestivamente le violazioni di dati personali, anche potenziali, di cui vengano a conoscenza.
2. La segnalazione deve essere effettuata trasmettendo il modulo allegato al presente Regolamento (Allegato 3) all'indirizzo *e-mail* privacy@asfo.sanita.fvg.it.

Articolo 7 – Segnalazione *data breach* esterni alla struttura

1. I Responsabili del trattamento (ditte appaltatrici, consulenti esterni, ecc.) sono tenuti a segnalare tempestivamente le violazioni di dati personali, anche potenziali, di cui vengano a conoscenza, trasmettendo il modulo allegato al presente Regolamento (Allegato 3) all'indirizzo *e-mail* privacy@asfo.sanita.fvg.it.

2. Ciascun Responsabile del trattamento che abbia trasmesso una segnalazione di *data breach* si mette a disposizione dell'Ufficio Privacy per ogni eventuale necessità e successiva indagine, anche *on site*, fornendo senza ritardo ogni informazione gli sia richiesta.
3. L'Autorità Giudiziaria e le Forze dell'Ordine segnalano fatti che possono configurare *data breach* tramite PEC all'indirizzo asfo.protgen@certsanita.fvg.it, *e-mail* all'indirizzo privacy@asfo.sanita.fvg.it o interlocuzione diretta con l'Ufficio Privacy.

CAPO IV – ISTRUTTORIA

Articolo 8 – Adozione di eventuali misure di sicurezza e istruttoria

1. Ricevuta la segnalazione di *data breach*, il Referente Privacy aziendale convoca tempestivamente l'Ufficio Privacy ed eventualmente il DPO e/o altre strutture aziendali competenti per specifici aspetti, ai fini dell'adozione di eventuali misure di sicurezza e dell'avvio dell'istruttoria.
2. L'istruttoria e le attività connesse sono effettuate all'insegna della massima tempestività.
3. Nelle more dell'accertamento del *data breach*, ove sussistano il *fumus boni iuris* (probabile esistenza del diritto di cui si chiede la tutela) e il *periculum in mora* (rischio che la mancata tempestività dell'azione cagioni un danno agli Interessati), il Referente Privacy aziendale propone sollecitamente al Titolare:
    - le misure tecniche e organizzative per porre rimedio alla violazione o attenuarne i possibili effetti negativi per gli Interessati e ridurre la probabilità che dalla violazione stessa derivino conseguenze lesive per gli Interessati o, comunque, scongiurare l'aggravarsi di tali conseguenze;
    - le misure tecniche e organizzative per prevenire simili violazioni future.
4. L'istruttoria ha ad oggetto:
    - i fatti/dati indicati nella sezione "Informazioni sulla violazione" del modulo per la notifica di violazioni di dati personali predisposto dal Garante per la Protezione dei Dati Personali;
    - i fatti/dati indicati nella sezione "Probabili conseguenze della violazione" del modulo per la notifica di violazioni di dati personali predisposto dal Garante per la Protezione dei Dati Personali;
    - le misure adottate o da adottare in seguito alla violazione (sezione "H" del modulo per la notifica di violazioni di dati personali predisposto dal Garante per la Protezione dei Dati Personali);
    - la valutazione del rischio per gli Interessati (sezione "I" del modulo per la notifica di violazioni di dati personali predisposto dal Garante per la Protezione dei Dati Personali).
5. La violazione di dati personali deve essere provata tramite uno o più mezzi di prova. Si applicano a riguardo, in quanto compatibili, le norme del codice civile che disciplinano i mezzi di prova.
6. A conclusione dell'istruttoria, l'Ufficio Privacy redige un apposito verbale, sulla base del modulo allegato (Allegato 4), in cui rappresenta i fatti/dati/misure/valutazioni indicati al precedente comma 4.
7. Il verbale è vistato dal DPO ed è tempestivamente trasmesso al Titolare, tramite l'Ufficio Protocollo.

CAPO VI – ANNOTAZIONE NEL REGISTRO DELLE VIOLAZIONI, NOTIFICHE E COMUNICAZIONI

Articolo 9 – Annotazione nel registro delle violazioni

1. L'Ufficio Privacy provvede ad annotare nel registro delle violazioni tanto gli incidenti di sicurezza (rischio probabile, ma non elevato per i diritti e le libertà degli interessati) e le violazioni di dati personali (rischio probabile ed elevato per i diritti e le libertà degli interessati), quanto gli eventi qualificati come irrilevanti a valle dell'istruttoria.
2. Il registro delle violazioni contiene:
    - numero identificativo e progressivo di valutazione dell'evento;
    - tipologia di segnalazione (Interessato / interna / esterna);
    - tipologia di violazione (riservatezza / integrità / disponibilità);
    - luogo dell'evento di violazione;
    - tipologia di dati personali violati;
    - cause della violazione;
    - qualificazione dell'evento (irrilevante / incidente di sicurezza / violazione di dati personali);
    - azioni immediate;
    - piano di intervento predisposto;
    - estremi della notifica;
    - estremi di comunicazione agli Interessati;
    - modalità di comunicazione agli Interessati;
    - motivazioni delle decisioni assunte.

Articolo 10 – Notifica all'Autorità Garante per la Protezione dei Dati Personali

1. L'Ufficio Privacy, entro 72 ore dall'invio al Titolare – tramite l'Ufficio Protocollo – del verbale di cui all'art. 8, ove ricorrano i presupposti di cui agli artt. 33 e 34 del GDPR, predispone, con il visto del DPO e a firma del Titolare, la notifica della violazione all'Autorità Garante per la Protezione dei Dati Personali, utilizzando il relativo modulo reperibile nel sito *web* del Garante medesimo.
2. La notifica è effettuata nelle modalità indicate nel sito stesso.
3. Qualora la notifica non sia effettuata entro le 72 ore dalla data indicata al precedente comma 1, deve essere accompagnata dalla descrizione delle ragioni del ritardo. È fatta comunque salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti, di cui il Titolare venga a conoscenza a seguito di ulteriori indagini e attività di *follow-up* (c.d. notifica per fasi).
4. In ogni caso, le ragioni del ritardo ovvero la scelta di non notificare l'evento devono essere documentate a cura dell'Ufficio Privacy.
5. In occasione della notifica, può richiedersi un parere all'Autorità Garante per la Protezione dei Dati Personali in ordine alla necessità o meno di effettuare anche una comunicazione nei confronti degli Interessati.

Articolo 11 – Notifica cumulativa

1. Il Titolare, qualora l'Azienda subisca in poco tempo violazioni della riservatezza multiple, riconducibili alla stessa tipologia (ad esempio molteplici attacchi informatici provenienti da un'unica fonte che colpiscono gli stessi applicativi) e/o che riguardino lo stesso tipo di dati personali di numerosi interessati, può non essere in condizioni di eseguire la notifica tempestiva all'Autorità Garante per la Protezione dei Dati Personali. In queste ipotesi, la scelta

più opportuna in termini di tempo e di efficacia può essere quella di eseguire una sola notifica avente a oggetto tutte le violazioni.

2. Qualora ricorrano i suddetti presupposti, l'Ufficio Privacy, con il visto del DPO, predispone, a firma del Titolare, l'eventuale notifica cumulativa tardiva, ossia oltre il termine delle 72 ore, purché corredata dei motivi del ritardo.

Articolo 12 – Notifica per fasi

1. È possibile che la fase istruttoria si prolunghi per un tempo tale da esporre i diritti o le libertà degli Interessati a un rischio di lesione. In questo caso, il Titolare del trattamento, su proposta dell'Ufficio Privacy e con il visto del DPO, provvede comunque alla notifica all'Autorità Garante, utilizzando lo strumento della c.d. notifica per fasi, indicando i motivi per i quali è necessario proseguire l'istruttoria e avvertendo della possibilità che la segnalazione si riveli infondata. Analogamente, procede con la comunicazione agli Interessati, con la precisazione che l'indagine sulla fondatezza della segnalazione è ancora in corso.

Articolo 13 – Comunicazione agli Interessati

1. Nel caso in cui il Titolare ritenga, sulla base dell'istruttoria condotta dall'Ufficio Privacy con il visto del DPO, che dal *data breach* possa derivare un rischio elevato per i diritti e le libertà degli Interessati coinvolti, questi devono essere informati senza ingiustificato ritardo, al fine di consentire loro di proteggersi dalle eventuali conseguenze negative della violazione.
2. Le modalità e i termini della comunicazione sono effettuati nel rispetto di quanto disciplinato dall'art. 34 del GDPR e tenendo conto delle eventuali indicazioni fornite dall'Autorità Garante per la Protezione dei Dati Personali.
3. La comunicazione deve contenere le seguenti informazioni:
    - la natura della violazione,
    - il nome e i dati di contatto del DPO e del Referente Privacy aziendale,
    - la descrizione delle probabili conseguenze;
    - la descrizione delle misure adottate, o di cui si propone l'adozione da parte del Titolare, per porre rimedio alla violazione dei dati personali o per attenuarne i possibili effetti negativi.
4. La comunicazione all'Interessato non è richiesta quando:
    - il Titolare – per il tramite degli Uffici aziendali competenti – abbia messo in atto tutte le misure tecniche e organizzative adeguate di protezione e tali misure siano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, come la cifratura;
    - il Titolare – per il tramite degli Uffici aziendali competenti – abbia successivamente adottato misure atte a scongiurare il sopraggiungere del rischio elevato per i diritti e le libertà degli Interessati;

oppure

    - la comunicazione richieda un impegno sproporzionato, potendosi, in tal caso, procedere ad una comunicazione pubblica o diffusa, tramite la quale gli Interessati siano informati con analoga efficacia.

CAPO VII – DISPOSIZIONI FINALI

Articolo 14 - Norma di rinvio

1. Per quanto non previsto nel presente Regolamento, trovano applicazione il GDPR e il d.lgs. n. 196/2003, così come modificato dal d.lgs. n. 101/2018, e loro eventuali modifiche e integrazioni.

Articolo 15 – Entrata in vigore

1. Il presente Regolamento si applica alle violazioni rilevate successivamente alla data di adozione dello stesso.
2. Del presente Regolamento è data pubblicità mediante la pubblicazione sul sito *internet* dell'Azienda, nella sezione Amministrazione Trasparente_ Disposizioni Generali_ Atti Generali_ Atti Amministrativi Generali_ Regolamenti.

ALLEGATO 1: Appendice normativa e regolamentare

Le fonti normative e regolamentari di riferimento per il presente Regolamento sono:

- Decreto Legislativo 10 agosto 2018, n. 101, "Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UR) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati";
- Regolamento (UE) n. 2016/679 del Parlamento Europeo del Consiglio del 24 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito, GDPR);
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i., "Codice per la protezione dei dati personali",
- WP250, "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679", adottate il 3 ottobre 2017 ed emanate il 06 febbraio 2018,
- Garante per la protezione dei dati personali, "Linee giuda in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul *web* da soggetti pubblici e da altri enti obbligati", provvedimento del 15 maggio 2014, di cui doc. *web* n. 3134436,
- Garante per la protezione dei dati personali, "Misure di sicurezza e modalità di scambio dei dati personali tra Amministrazioni Pubbliche", provvedimento del 2 luglio 2005, di cui al doc. *web* n. 4129029,
- Decreto legislativo 7 marzo 2005, n. 82 e s.m.i., "Codice dell'Amministrazione Digitale (CAD)",
- Codice di Procedura Penale, art. 331 (Denuncia da arte di pubblici ufficiali e incaricati di pubblico servizio), art. 361 (Omessa denuncia di reato da parte di pubblico ufficiale),
- Decreto del Ministero degli Interni in attuazione della Legge 31 luglio 2005, n. 155, sulle infrastrutture critiche,
- Decreto del Presidente del Consiglio dei Ministri del 1 aprile 2008, "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'art. 71, comma 1-*bis* del decreto legislativo 7 marzo 2005, n. 82, recante il 'Codice dell'Amministrazione Digitale (CAD)'",
- Decreto del Presidente del Consiglio dei Ministri del 24 ottobre 2014, "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale dei cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle Pubbliche Amministrazioni e delle imprese",
- Decreto del Direttore Generale n. 723 del 26.11.2020, recante "Regolamento per la protezione dei dati personali dell'Azienda sanitaria Friuli Occidentale";
- *Guidelines 01/2021 on Examples regarding Data Breach Notification* del 2.03.2021;
- Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali del 27.05.2021 recante "Procedura telematica per la notifica di violazioni di dati personali".

ALLEGATO 2: Registro delle violazioni

ID evento	**TIPOLOGIA** di segnalazione (Interessato / interna / esterna)	**VIOLAZIONE** di*			**LUOGO** della violazione	**TIPOLOGIA** dei dati personali violati	**CAUSE** della violazione**	**QUALIFICAZIONE** dell'evento***			**AZIONI** immediate	**PIANO D'INTERVENTO** predisposto	**ESTREMI** della notifica al Garante	**ESTREMI** della comunicazione agli Interessati	**MODALITà** della comunicazione agli Interessati	**MOTIVAZIONE** delle decisioni assunte		
		R	I	D				Ø	IS	V						NON si notifica al Garante	RITARDO nella notifica al Garante	NON si comunica agli Interessati

* Violazione di:
R = riservatezza
I = integrità
D = disponibilità

** Classificazione delle cause di *data breach*:
1 = hackeraggio
2 = *malware*
3 = cattivo uso dei *social*
4 = errore umano o disattenzione
5 = cattivo uso della tecnologia
6 = fisico
7 = ambientale

*** Qualificazione dell'evento:
Ø = irrilevante
IS = incidente di sicurezza
V = violazione di dati

ALLEGATO 3: Modulo per la segnalazione di un sospetto *data breach*

MODULO PER LA SEGNALAZIONE DI UN SOSPETTO CASO DI *DATA BREACH*

Al Referente aziendale *privacy*
privacy@asfo.sanita.fvg.it

Il Responsabile del trattamento / Il Delegato al trattamento / L'Autorizzato al trattamento / L'Interessato

_____ tel. _____
(nome e cognome)

_____
(se Delegato o Autorizzato: incarico/ funzione ricoperti)

_____
(se ditta esterna: denominazione ditta)

_____
_____
(se Interessato: codice fiscale, tipologia e n. documento di identità)

comunica che si è verificata una possibile violazione di dati.

Data evento:

- Il giorno _____
- Tra il giorno _____ e il giorno _____
- Dal giorno _____ a tutt'oggi
- In un tempo / periodo che non è ancora stato possibile determinare

Ulteriori informazioni circa le date in cui è avvenuta la violazione:
_____
_____
_____

Luogo evento (puntualmente determinato: stanza ambulatorio, auto di servizio, ecc.):
_____
_____
_____

Natura della violazione:

- perdita di riservatezza
- perdita di integrità
- perdita di disponibilità

Descrizione della violazione:

- distruzione/cancellazione (i dati non sono più nei sistemo gestiti dal Titolare e non li ha può neppure l'autore della violazione, con impossibilità di recupero),
- perdita/smarrimento
- modifica
- divulgazione non autorizzata
- accesso non autorizzato
- lettura
- estrazione di copia (i dati sono ancora presenti nei sistemi del Titolare)
- alterazione (i dati sono presenti nei sistemi del Titolare ma risultano alterati)
- altro: _____

Causa della violazione:

- azione intenzionale interna alla struttura del Titolare
- azione accidentale interna alla struttura del Titolare
- azione intenzionale esterna alla struttura del Titolare
- azione accidentale esterna alla struttura del Titolare

Dispositivo/sistema oggetto della violazione:

- *Computer* personale (indirizzo IP, nome macchina o altro identificativo univoco del dispositivo _____)
- Dispositivo mobile (*computer* portatile o cellulare) in carico a:
  _____
  _____
- *Software*: _____
- *File* o parte di *file* (percorso di archiviazione informatica):
  _____
  _____
- Documento cartaceo (dove era archiviato il documento: scrivania, cassetto, armadio, ecc.):
  _____
  _____
- Altro: _____
  _____

Categorie di interessati coinvolti nella violazione:

- dipendenti/consulenti/collaboratori
- utenti/assistiti
- sostenitori (es. donanti)

- soggetti che ricoprono cariche sociali
- minori
- persone vulnerabili
- altro: _____

Quantità di persone colpite dalla violazione:

- n. _____
- circa n. _____
- n. ancora sconosciuto di persone
- n. non determinabile

Descrizione sommaria dei dati oggetto della violazione (personali, banca dati, documentali, dati crittografati, ecc.):

_____
_____
_____

Categorie di dati oggetto della violazione:

- dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
- dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- dati di accesso e di identificazione (username, password, customer ID, altro)
- dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
- dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro)
- dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
- dati di profilazione
- dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro)
- dati relativi all'ubicazione
- dati che rivelano l'origine razziale o etnica
- dati che rivelano le opinioni politiche
- dati che rivelano le convinzioni religiose o filosofiche
- dati che rivelano l'appartenenza sindacale
- dati relativi alla vita sessuale o all'orientamento sessuale
- dati relativi alla salute
- dati genetici
- dati biometrici
- altro: _____
- categorie ancora non determinate

Quantità di registrazioni dei dati personali oggetto di violazione:

- n. _____
- circa n. _____

- n. ancora sconosciuto di persone
- n. non determinabile

Misure tecniche e organizzative applicate ai dati oggetto di violazione (chiusura porta, chiusura a chiave armadio, crittografia dei dati, ecc.):

_____
_____

Probabili conseguenze della violazione per gli Interessati:

→ in caso di perdita di riservatezza:
- i dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
- i dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
- i dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
- altro: _____
  _____

→ in caso di perdita di integrità:
- i dati sono stati modificati e resi inconsistenti
- i dati sono stati modificati mantenendo la consistenza
- altro: _____

→ in caso di perdita di disponibilità:
- mancato accesso a servizi
- malfunzionamento e difficoltà nell'utilizzo di servizi
- altro: _____

Ulteriori considerazioni sulle probabili conseguenze:

_____
_____
_____

Potenziale impatto per gli Interessati:
- perdita del controllo dei dati personali
- limitazione dei diritti
- discriminazione
- furto o usurpazione d'identità
- frodi
- perdite finanziarie
- decifratura non autorizzata della pseudonimizzazione
- pregiudizio alla reputazione
- perdita di riservatezza dei dati personali protetti da segreto professionale

- conoscenza da parte di terzi non autorizzati
- qualsiasi altro danno economico o sociale significativo:
  _____
  _____
- non ancora definito

Gravità del potenziale impatto per gli Interessati:

- trascurabile
- bassa
- media
- alta
- non ancora definita

Motivazioni:

_____
_____
_____

Il sottoscritto resta a disposizione per ogni ulteriore chiarimento che si rendesse necessario.

Luogo e data, _____

Firma_____

ALLEGATO 4: Schema di verbale di accertamento di *data breach*

PROT. N.
DATA

Azienda sanitaria Friuli Occidentale
Via della Vecchia Ceramica n. 1
33170 – Pordenone

Dall'istruttoria condotta a seguito della segnalazione prot. n. _____ del _____, è emerso che:

- la violazione è avvenuta (data) _____, in (luogo) _____.
- La violazione si è tradotta in una perdita di riservatezza / integrità / disponibilità, in quanto si è verificata una (descrizione della violazione) _____ dei dati, a causa di _____.
- La violazione ha interessato (indicare dispositivo/sistema) _____ _____ e coinvolto (quantità e tipologie di Interessati) _____.
- I dati violati rientrano nelle seguenti categorie:
  _____
  _____
  _____, per (numero) _____ registrazioni.
- Le misure tecniche e organizzative già adottate al momento della segnalazione erano le seguenti:
  _____
  _____
  _____.

Si ritiene che le probabili conseguenze della violazione, per gli Interessati, possano essere
_____
_____
_____,
con potenziale trascurabile/basso/medio/alto impatto su _____
_____
_____,
per le seguenti ragioni _____
_____
_____.

A seguito della segnalata violazione, sono state adottate/si propone l'adozione delle seguenti misure di sicurezza tecniche e organizzative per porre rimedio alla violazione stessa e attenuarne i possibili effetti negativi: _____
_____
_____.

Per prevenire simili violazioni in futuro, sono state adottate/si propone l'adozione delle seguenti misure di sicurezza tecniche e organizzative: _____
_____
_____.

Tutto ciò premesso, si ritiene che la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche/la violazione non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche/siano necessari ulteriori elementi per effettuare la valutazione del rischio per i diritti e le libertà delle persone fisiche.

In fede,

Il Data Protection Officer AsFO
_____

Il Referente Privacy aziendale
_____

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: RICCARDO MARIO PAOLI
CODICE FISCALE: PLARCR66T09A271S
DATA FIRMA: 14/12/2021 17:01:55
IMPRONTA: 3B69C9B3441B032A09E2A4D8A34A8ACACC673AB37820982680309551F2EADA00
CC673AB37820982680309551F2EADA00760CC3378E73EEF49400DFD0F733FA9A
760CC3378E73EEF49400DFD0F733FA9A1ED43C0F59F888635894ADDF00097755
1ED43C0F59F888635894ADDF00097755343B39707E8C8503BDD4E930A9CFDD78

NOME: MICHELE CHITTARO
CODICE FISCALE: CHTMHL71R31L483A
DATA FIRMA: 14/12/2021 17:27:24
IMPRONTA: 79C38B60CAC5DF06A6EC01FC027629105D9D8978C52B5B8BC5917073C592D83A
5D9D8978C52B5B8BC5917073C592D83ABE5A31B6AAB4E17032CFEE9E3B15B51E
BE5A31B6AAB4E17032CFEE9E3B15B51EB8A21D8486AF11E4484B06E0C7C87EDC
B8A21D8486AF11E4484B06E0C7C87EDC02A4366954F0509F2BAFAF7D5BDC7409

NOME: CARLO FRANCESCUTTI
CODICE FISCALE: FRNCRL60H19B940W
DATA FIRMA: 14/12/2021 17:47:06
IMPRONTA: 546F2AE86C178F309A1E95F76D4C72CC8E05511346A2065B2F63AD6ED5651221
8E05511346A2065B2F63AD6ED56512214FEB712C698FECA8CE8A13083F35F7F0
4FEB712C698FECA8CE8A13083F35F7F08044094485666AE63C15EEFB31A70BE3
8044094485666AE63C15EEFB31A70BE3822BFAC411008AF6D76498C22CBAEEFE

NOME: JOSEPH POLIMENI
CODICE FISCALE: PLMJPH69D21Z404X
DATA FIRMA: 14/12/2021 17:57:36
IMPRONTA: 35E5380CD6E75268DBD9CA9AB04F22B1A7B6F614D5D4A69BE3CAB1D5A7F4A703
A7B6F614D5D4A69BE3CAB1D5A7F4A703DA1540229CFC653470412DD2DE02AE87
DA1540229CFC653470412DD2DE02AE87BEACE58A080F563AF32FE6DC376FD659
BEACE58A080F563AF32FE6DC376FD6594C69F69F7E28A59762E07F88D4A5E8E9