

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO

(Dott. Antonio Battistini)
(D.C.A. n. 25 del 29 gennaio 2024)

N. 1311 DEL 17/10/2024

<u>OGGETTO:</u>	ADEMPIMENTI IN APPLICAZIONE DELL'ART.33 DEL REGOLAMENTO GENERALE UE PROTEZIONE DATI N. 2016/679 ED IN APPLICAZIONE DEGLI ARTT. 3 E 4 DPCM N. 81/2021. REGOLAMENTO PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI E DELLE NOTIFICHE DEGLI INCIDENTI AVENTI IMPATTO SUI BENI ICT.
------------------------	---

STRUTTURA PROPONENTE	Direzione Amministrativa
-----------------------------	---------------------------------

Parere Direttore Amministrativo Dott. TIZIANA CIUCI (Sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.)	<i>Favorevole</i>
--	-------------------

Parere Direttore Sanitario Dott. ANTONIO GALLUCCI (Sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.)	<i>Favorevole</i>
--	-------------------



*Dipartimento Tutela della Salute
e Politiche Sanitarie*

AZIENDA SANITARIA PROVINCIALE CATANZARO



REGIONE CALABRIA

OGGETTO:	ADEMPIMENTI IN APPLICAZIONE DELL'ART.33 DEL REGOLAMENTO GENERALE UE PROTEZIONE DATI N. 2016/679 ED IN APPLICAZIONE DEGLI ARTT. 3 E 4 DPCM N. 81/2021. REGOLAMENTO PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI E DELLE NOTIFICHE DEGLI INCIDENTI AVENTI IMPATTO SUI BENI ICT.
-----------------	---

Proposta del Responsabile del Procedimento n.6788 / 2024

Il Responsabile del Procedimento con la sottoscrizione del presente atto, a seguito dell'istruttoria fatta, attesta che l'atto è conforme alla legge.

Il Responsabile del Procedimento
GIUSEPPE COZZA D'ONOFRIO

Il Direttore Amministrativo Aziendale	Dott.ssa TIZIANA CIUCI (Sottoscritto digitalmente ai sensi dell'art. 21 D.Lgs n. 82/2005 e s.m.i.)
--	--

Il Direttore Amministrativo Aziendale

Visto il D.C.A. n. 25 del 29 gennaio 2024 con il quale il Dott. Antonio Battistini è stato confermato, ai sensi dell'art. 2, comma 1, del decreto legge n.150 del 10 novembre 2020, convertito con modificazioni nella legge 30 dicembre 2020, n.181 e s.m.i, Commissario Straordinario dell'Azienda Sanitaria Provinciale di Catanzaro;

Vista la Deliberazione del Commissario Straordinario n.701 del 13 giugno 2023;

Vista la deliberazione del Commissario Straordinario n.865 del 14 luglio 2023;

PREMESSO CHE

il Regolamento (UE) 2016/679 del Parlamento e del Consiglio Europeo del 27 aprile 2016 disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali (in breve RGPD);

Visti

l'art. 33 del suddetto RGPD 2016/679 che così dispone: "In caso di violazioni di dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55, senza ingiustificato ritardo e, ove possibile, entro le 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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo";

- le Linee Guida del Gruppo ex art. 29 n. 250 del 3 ottobre 2017, emendate in data 6 febbraio 2018, che illustrano gli obblighi di notifica e di comunicazione in caso di violazioni dei dati

Proposta n. 6788/2024

personali, ai sensi del Regolamento EU 2016/679 e forniscono inoltre alcuni esempi dei vari tipi di violazione;

- il decreto del presidente del consiglio dei ministri 14 aprile 2021, n. 81 contenente la disciplina in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici;
- l'art. 3 del decreto del presidente del consiglio dei ministri 14 aprile 2021, n. 81 che obbliga i soggetti inclusi nel perimetro di sicurezza, al verificarsi di uno degli incidenti avente impatto su un bene ICT, di procedere alla notifica al CSIRT.
- l'art. 4 del decreto del presidente del consiglio dei ministri 14 aprile 2021, n. 81 il quale prevede che i soggetti inclusi nel perimetro di sicurezza possano effettuare la notifica su base volontaria degli incidenti relativi ai beni ICT, nei casi ivi previsti;

Preso atto che

con deliberazione n. 246 del 16.02.2024 è stato costituito un Gruppo di Lavoro Privacy ai sensi dell'art. 2-quaterdecies del D.lgs. n.196/2003 (Codice Privacy), al fine di garantire, interfacciandosi con il DPO, il pieno assolvimento degli obblighi previsti dalla normativa vigente in materia di protezione dei dati personali;

Ritenuto opportuno

doversi adottare un Regolamento Aziendale per la corretta gestione delle violazioni dei dati personali e delle notifiche degli incidenti aventi impatto sui beni ICT;

Richiamato il vigente Regolamento di Organizzazione e Funzionamento Aziendale e ritenuta la propria competenza;

Visti gli esiti del procedimento istruttorio espletato dal Responsabile del procedimento designato ai sensi della Legge 241/90 e s.m.i.

PROPONE

Per quanto esposto in narrativa che qui si intende integralmente ripetuto e confermato:

1. di approvare il regolamento da utilizzare in caso di violazione di dati personali (Data breach) e per le notifiche degli incidenti aventi impatto sui beni ICT, qui allegato, per costituirne parte integrante;
2. di delegare il Coordinatore del Gruppo Privacy e, in sua assenza, il vice Coordinatore del Gruppo Privacy, ad inoltrare la notifica al Garante di cui all'art. 33 del RGPD, nei casi in cui sarà necessario;
3. di delegare il Coordinatore del Gruppo Privacy e, in sua assenza, il vice Coordinatore del Gruppo Privacy, ad inoltrare la notifica al CSIRT di cui agli artt. 3 e 4 DPCM n. 81/2021, nei casi previsti;

4. di dare mandato al Responsabile URP per la pubblicazione del Regolamento sul portale aziendale con valore di notifica ;
5. di comunicare il presente atto al DPO Aziendale, Ing. Mario Pastore, della Soc. Liguria Digitale; ;
6. di dare atto che il presente provvedimento non comporta onere di spesa a carico del bilancio aziendale;
7. di Trasmettere il presente atto, ai Designati del Trattamento dei Dati Personali, al Gruppo di Lavoro Privacy ,al Responsabile URP;
8. di pubblicare il presente atto in “Amministrazione Trasparente Sezione Regolamenti”.

IL COMMISSARIO STRAORDINARIO

Sulla base della proposta del Direttore Amministrativo;

ACQUISITI i pareri espressi dal Direttore Amministrativo e dal Direttore Sanitario per quanto di rispettiva competenza;

DELIBERA

Di far propria la proposta, che qui si intende integralmente riportata e trascritta, per come sopra formulata.

IL COMMISSARIO STRAORDINARIO

Dott. Antonio Battistini

(Sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

REGOLAMENTO AZIENDALE

PER LA CORRETTA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI E DELLE NOTIFICHE DEGLI INCIDENTI AVENTI IMPATTO SUI BENI ICT

art. 33 del Regolamento (UE) 2016/679 DPCM n. 81/2021

REGOLAMENTO AZIENDALE

PER LA CORRETTA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI E DELLE NOTIFICHE DEGLI INCIDENTI AL CSIRT ITALIA

ai sensi dell'art. 33 del Regolamento (UE) 2016/679 e degli artt. 3 e 4 DPCM n. 81/2021

SOMMARIO

1. PREMESSA.....	3
2. SCOPO E CAMPO DI APPLICAZIONE.....	4
3. NORMATIVA DI RIFERIMENTO.....	5
4. DEFINIZIONI.....	7
5. NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).....	9
6. NOTIFICA DI UN INCIDENTE AVENTE IMPATTO SU BENI ICT.....	10
7. COMUNICAZIONE AGLI INTERESSATI.....	11
8. POSSIBILI SCENARI DATA BREACH.....	11
9. GESTIONE DEGLI INCIDENTI AVENTI IMPATTO SUI BENI ICT.....	13
10 ESEMPI DI INCIDENTI DI SICUREZZA.....	15
11. REGISTRO DELLE VIOLAZIONI.....	16
ALLEGATO 1 –	17
ALLEGATO 2 – COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO.....	18
ALLEGATO 3 – REGISTRO DELLE VIOLAZIONI.....	19
ALLEGATO 4 TASSONOMIA DEGLI INCIDENTI	20

1. PREMESSA

Una violazione dei dati personali (c.d. *data breach*) può scaturire sia dall'interno che dall'esterno dell'Azienda e, se non affrontata in modo adeguato e tempestivo, può provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il regolamento generale sulla protezione dei dati introduce l'obbligo di notificare una violazione dei dati personali (di seguito "violazione") all'autorità di controllo nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

I possibili scenari di violazione dei dati sono sicuramente aumentati con l'avvento della società digitale. Gli operatori devono, pertanto, sviluppare la capacità di riconoscere ed affrontare le potenziali conseguenze, ad esempio sulle cure di un paziente, di eventi pregiudizievoli quali un accesso non autorizzato (hackeraggio o cessione di credenziali, furto di appunti sulle password), una modifica erronea di un database, un malfunzionamento di uno strumento informatico o il furto o perdita di un dispositivo (smartphone o chiavetta USB, telefonino aziendale) contenente dati di estrema delicatezza (dati sullo stato di salute), o la comunicazione di dati attraverso strumenti a larga diffusione (invio massivo di email o pubblicazione dati sul web).

In accordo con il principio di responsabilizzazione, di cui all'art. 5 del GDPR, la diffusione del presente regolamento viene assicurato attraverso:

- la pubblicazione sul Sito internet nella sezione Privacy/Regolamenti;
- trasmissione ai Direttori/Dirigenti della Strutture Aziendali e, per il loro tramite al personale in esse operante per informarlo ed istruirlo in merito alle azioni da porre in essere nel caso di violazioni.

La mancata segnalazione di una violazione può comportare l'imposizione di una sanzione al Direttore della U.O.C./ Responsabile della U.O.S.D./Responsabile unità.

2. SCOPO E CAMPO DI APPLICAZIONE

Lo scopo del presente regolamento è:

1. Definire, nel rispetto della normativa di riferimento, le modalità operative per una corretta e tempestiva gestione delle violazioni dei dati personali trattati dall' Azienda Sanitaria Provinciale di CZ (di seguito per brevità "Titolare");
2. Definire i ruoli e le responsabilità organizzative per la gestione di un data breach;
3. Assicurare un servizio essenziale per il mantenimento di attività fondamentali per l'interesse dello Stato di cui all'art. 1, co. 2, lett. a), n. 1 e n. 2, D.L. n. 105/2019).

Pertanto, con il presente documento si definiscono e regolamentano:

- le modalità operative per la tempestiva segnalazione al Gruppo Privacy dell'eventuale violazione per il tramite del referente Privacy;
- i processi da mettere in atto per essere in grado di rilevare e limitare tempestivamente gli effetti di una violazione di dati personali;
- le modalità e i criteri per l'eventuale comunicazione alle persone fisiche interessate, ove necessario;
- le modalità operative per la tempestiva notifica al CSIRT da parte del Coordinatore Gruppo Privacy.
- le modalità operative e i criteri per la tempestiva notifica all'Autorità di controllo (Garante Privacy) da parte del Coordinatore Gruppo Privacy.

La presente procedura si applica a:

1. tutte le Strutture dell'Azienda che trattano, a qualsiasi titolo (dipendenti, universitari, borsisti, tirocinanti.) e in qualsiasi modalità (automatizzata, manuale, digitale, cartacea), dati e informazioni all'interno dell'Azienda, nonché ai Responsabili esterni di trattamento di cui all'art. 28 del GDPR che trattano i dati per conto del Titolare;
2. tutti i beni ICT dell'Azienda.

Il presente regolamento è rivolto a:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare (di seguito "destinatari interni");
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dai destinatari interni che, in ragione del rapporto contrattuale in essere con il Titolare abbia accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare, e agisca in qualità di Responsabile del trattamento art. 28 del Regolamento o di autonomo Titolare del trattamento (di seguito "destinatari esterni");
- qualsiasi soggetto (persona fisica o persona giuridica) che a qualsiasi titolo e quindi a prescindere dal tipo di rapporto intercorrente con il Titolare, rilevano un incidente avente impatto su un bene ICT di rispettiva pertinenza appartenente alla tassonomia in allegato.

Di seguito definiti per semplicità "Soggetto segnalante".

Tutti i destinatari, quindi interni ed esterni, devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione. Tale Regolamento viene pertanto pubblicato sul sito istituzionale nonché nella sez. Amministrazione Trasparente.

3. NORMATIVA DI RIFERIMENTO

- Regolamento (UE) 2016/679 del Parlamento Europeo 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento).
- Decreto Legislativo 10 agosto 2018 n. 101 "Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 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 e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)"
- Linee guida in materia di notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 - WP250rev.01.
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019.
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015, come modificata Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951]
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951]
- D.Lgs. 82/2005 Codice dell'Amministrazione Digitale (CAD)
- artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale)
- Direttiva (UE) 2016/1148 (Direttiva NIS) del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Europea
- Prescrizione del WP29 "Guidelines on Personal data breach notification under Regulation 2016/679, adottate il 03.10.2017 (ultima revisione 06/02/2018)
- Prescrizione del WP29 "Guidelines on Personal data breach notification under Regulation 2016/679, adottate il 03.10.2017 (ultima revisione 06/02/2018)
- Decreto Legislativo 18 maggio 2018 n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
- Decreto-legge n.82 del 14 giugno 2021, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale

- LEGGE 28 giugno 2024, n. 90 Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici
- DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 14 aprile 2021, n. 81, Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.
- Guida Alla Notifica Degli Incidenti al Csirt Italia-Agenzia Per La Cybersicurezza Nazionale

4. DEFINIZIONI

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 (art. 4, punto 1 del Regolamento).

Trattamento: 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 (art. 4, punto 2).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

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 (art. 4, punto 7 del Regolamento). In questo contesto, è titolare del trattamento ASP IIAARR.

Gruppo di Lavoro Privacy : le persone fisiche individuate dal Titolare ai sensi dell'art. 2-quaterdecies del D.lgs. n.196/2003 (Codice Privacy) che, interfacciandosi con il DPO, garantiscono il pieno assolvimento degli obblighi previsti dalla normativa vigente in materia di protezione dei dati personali.

Referente privacy: la persona fisica afferente ad una UdO che operativamente supporta il direttore/responsabile nell'attuazione delle policy di privacy.

Regolamento o GDPR: Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016 679)

Responsabile Protezione Dati o Data Protection Officer: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del Regolamento (in particolare artt. 37, 38, 39 del Regolamento).

Designato al trattamento: La persona fisica che opera sotto l'autorità e responsabilità del titolare del trattamento, al quale possono essere delegati ai sensi dell'art. 2-quaterdecies del D.lgs. n.196/2003 (Codice

Privacy) specifici compiti e funzioni e, secondo l'organizzazione aziendale, determina specifiche modalità organizzative rispetto ad uno o più trattamenti.

Autorizzato al trattamento o incaricato al trattamento: La persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali.

Responsabile esterno 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 (art. 4, punto 8 del Regolamento).
Violazione dei dati personali (c.d. 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 (art. 4, punto 12 del Regolamento).

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 (art. 4, punto 12 del Regolamento)

Incidente di sicurezza: Evento singolo o in serie di eventi di eventi non voluti o inaspettati che ha una probabilità significativa di compromettere il funzionamento di processi aziendali e minacciare la sicurezza informativa.

bene ICT: (information and communication technology), un insieme di reti, sistemi informativi e servizi informatici, o parti di essi,

Incidente: ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici" (art. 1, comma 1, lett. h) del DPCM n. 81/2021)

CSIRT Italia: è il centro operativo all'interno dell'Agenzia per la Cybersicurezza Nazionale (ACN) incaricato delle azioni di preparazione, prevenzione, gestione e risposta a eventi ed incidenti cibernetici(<https://www.csirt.gov.it>)

5. NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

In caso di violazione dei dati personali il **soggetto segnalante** avverte immediatamente il Gruppo Privacy dell'avvenuta violazione.

Il Coordinatore del Gruppo Privacy mette a conoscenza tempestivamente il DPO utilizzando gli appositi dati di contatto (posta elettronica e telefono).

La notifica deve essere trasmessa dal soggetto segnalante al Gruppo Privacy utilizzando il modello allegato al presente regolamento (Allegato 1) per mezzo di posta elettronica, anticipandola telefonicamente ai Direttori/Responsabili delle Unità Operative interessate.

La stessa notifica deve essere trasmessa, per conoscenza, anche al Responsabile della Protezione dei Dati (DPO) dal Coordinatore del Gruppo Privacy.

Il Coordinatore del Gruppo Privacy, in qualità di delegato dal Titolare, dovrà notificare, sentito il parere del DPO, la violazione all'autorità di controllo (Garante per la protezione dei dati personali), e in qualità di delegato dal Titolare, in accordo a quanto disciplinato dalla normativa vigente in materia di cybersecurity, notifica l'incidente avente impatto su un bene ICT al **CSIRT** secondo le modalità e le tempistiche definite nei punti seguenti.

La mancata segnalazione di una violazione può comportare l'imposizione di una sanzione al Direttore della U.O.C./ Responsabile dell'unità.

6. NOTIFICA DI UN INCIDENTE AVENTE IMPATTO SU BENI ICT

In caso di incidente avente impatto su un bene ICT di rispettiva pertinenza, **Il soggetto segnalante** avverte immediatamente il Gruppo Privacy dell'avvenuta violazione.

Il Coordinatore del Gruppo Privacy mette a conoscenza tempestivamente il DPO utilizzando gli appositi dati di contatto (posta elettronica e telefono).

Il soggetto segnalante notifica l'incidente avente impatto sui beni ICT utilizzando il modello allegato al presente regolamento (Allegato 1) per mezzo di posta elettronica, anticipandola telefonicamente:

- al Direttore GTP in caso di violazione di dati gestiti su sistemi informatici o analogici;

La stessa notifica deve essere trasmessa, per conoscenza, anche al Responsabile della Protezione dei Dati (DPO) dal Coordinatore del Gruppo Privacy.

Il Coordinatore del Gruppo Privacy, in qualità di delegato dal Titolare in accordo a quanto disciplinato dalla normativa vigente in materia di cybersecurity, notifica gli incidenti al CSIRT secondo le modalità definite al punto 9 "gestione degli incidenti aventi impatto sui beni ict" e in accordo alle seguenti tempistiche, e meglio illustrate nella tabella a seguire:

- 1 ora** per gli incidenti di cui alla Tabella 2 dell'allegato A del DPCM 81/2021 (incidenti ICPB);
- 6 ore** per gli incidenti di cui alla Tabella 1 dell'allegato A del DPCM 81/2021 (incidenti ICPA). Per gli incidenti con impatti su reti, sistemi informativi e servizi informatici diversi dai beni ICT (art. 1, co. 3-
- Segnalazione entro 24 ore e relativa notifica completa entro 72 ore** (incidenti ICP-C)

TIPOLOGIA DI EVENTO	IDENTIFICAZIONE DELL'ASSET	CLASSE IDENTIFICATIVA INCIDENTE	TIPO DI NOTIFICA	TEMPISTICHE
Incidente che rientra nelle classificazioni della tassonomia	BENE ICT O CONTIGUO	ICP-B	OBBLIGATORIA	ENTRO 1 ORA dal rilevamento dell'incidente
Incidente che rientra nelle classificazioni della tassonomia	BENE ICT O CONTIGUO	ICP-A	OBBLIGATORIA	ENTRO 6 ORE dal rilevamento dell'incidente
Incidente che rientra nelle classificazioni della tassonomia	DIVERSO DA BENE ICT	ICP-C	OBBLIGATORIA	Segnalazione: ENTRO 24 ORE Notifica: ENTRO 72 ORE dal rilevamento dell'incidente
incidente che rientra nelle classificazioni della tassonomia	DIVERSO DA BENE ICT E DA BENE CONTIGUO	ICP-A/B	VOLONTARIA	NESSUNA TEMPISTICA
Incidente che non rientra nelle classificazioni della tassonomia	BENE ICT	-	VOLONTARIA	NESSUNA TEMPISTICA

7. COMUNICAZIONE AGLI INTERESSATI

Nel caso, e solo nel caso, in cui dal *data breach* (**violazione di dati personali**) possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate, senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

L'eventuale comunicazione all'interessato/agli interessati (Allegato 2), a firma del Coordinatore del Gruppo Privacy, in qualità di delegato dal titolare, deve inviarsi nei tempi e nei modi che lo stesso individuerà come più opportuno e come specificato nell'art. 34 del Regolamento e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante per la protezione dei dati personali

8. POSSIBILI SCENARI DATA BREACH

Vanno notificate all'Autorità Garante unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.

Ciò può includere, ad esempio, la perdita del controllo sui dati personali dei pazienti, dei lavoratori, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti (es. dati idonei a rilevare lo stato di salute), una perdita, un danno alla vita privata dei pazienti e qualsiasi altro significativo svantaggio economico o sociale.

Di seguito sono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella valutazione in merito alla necessità di effettuare o meno la notifica di *data breach* all'Autorità Garante.

Tipi di violazioni dei dati personali:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Le violazioni, secondo le indicazioni fornite dal Gruppo di Lavoro art. 29, possono manifestarsi in diversi modi ed essere classificate in tre tipologie:

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

A seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

L'articolo 32 del "Regolamento" dispone che il Titolare del trattamento, nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, deve tenere conto, tra le altre cose, "della capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

In caso di violazione dei dati personali, il Titolare del Trattamento deve, art. 33 del Regolamento, notificare all'autorità di controllo (Garante Privacy) la violazione senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Ne deriva che la notifica dell'avvenuta violazione al Garante non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati. Se la probabilità del rischio è elevata, dovranno essere informati anche gli interessati.

Il criterio dirimente per valutare la necessità di avviare una procedura di notifica è pertanto la probabilità che l'incidente di sicurezza possa porre a rischio (per la notifica all'Autorità), o ad elevato rischio (per la comunicazione agli interessati) le libertà e i diritti degli individui.

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione da notificare al Garante e comunicare agli interessati solo qualora la mancanza di accesso alle informazioni può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche.

Non configura invece una "violazione della sicurezza" l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata se accompagnata da opportune misure organizzative tese a salvaguardare i diritti e le libertà fondamentali.

Il Titolare ha il dovere di notificare al Garante nei seguenti casi:

- l'organizzazione è Titolare del/i trattamenti dei dati coinvolti nell'incidente
- l'organizzazione è Contitolare del trattamento con delega alla notifica

Gli incidenti di sicurezza occorsi, anche se non notificate al Garante e non comunicate agli interessati devono essere registrate, analizzate e archiviate a cura del Gruppo Privacy.

9. GESTIONE DEGLI INCIDENTI AVENTI IMBATTO SUI BENI ICT

Fase 1 – Notifica da parte del soggetto segnalante al Coordinatore del Gruppo Privacy

Il soggetto segnalante dovrà compilare l'apposito modulo e fornire ove possibile le seguenti informazioni:

- tipologia di impatto, distinta tra: o impatto su bene ICT , su bene contiguo o su altri beni;
- date e ora di rilevamento dell'incidente;
- ulteriori dettagli dell'incidente, come ad esempio altri sistemi impattati o informazioni rilevanti;

Il soggetto segnalante dovrà trasmettere il modulo al Coordinatore del Gruppo Privacy per mezzo posta elettronica e avvertirlo immediatamente con comunicazione telefonica.

In sua assenza dovrà avvertire il Direttore della S.C. Sistemi Informativi con le stesse modalità.

La mancata segnalazione di una violazione può comportare l'imposizione di una sanzione al Direttore della U.O.C./ Responsabile dell'unità.

Fase 2 –Notifica dell'incidente da parte del Gruppo Privacy al CSIRT

il Coordinatore del Gruppo Privacy o in sua assenza, il Direttore della U.O.C. GTP dovrà, secondo i tempi previsti dalla normativa vigente, compilare l'apposito modulo disponibile online sul sito internet del CSIRT Italia (<https://www.csirt.gov.it/segnalazione>) e fornire le seguenti informazioni:

- tipologia di impatto, distinta tra: o impatto su bene ICT (notifica art.3, comma 1 DPCM n. 81/2021);
- impatto su bene contiguo (notifica art.3, comma 3 DPCM n. 81/2021); o impatto su altri beni (notifica art.1, comma 3-bis D.L. n.105/2019); o impatto per cui non sussiste un obbligo di notifica (art.4 DPCM n. 81/2021);
- date e ora di rilevamento dell'incidente; ulteriori dettagli dell'incidente, come ad esempio altri sistemi impattati o informazioni rilevanti;

Attività necessarie e propedeutiche alla notifica al CSIRT:

identificazione delle reti, dei sistemi informativi e servizi informatici impattati dall'incidente;

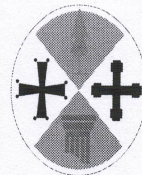
identificazione della tipologia di incidente da segnalare in accordo alla tassonomia degli incidenti di cui all'Allegato A del DPCM n. 81/2021 e di quella di cui all'Allegato A alla DETERMINA ACN del 3 gennaio 2023.

Attività a supporto della notifica al CSIRT:

raccolta delle evidenze (es. IOC, evidenze, azioni di ripristino) relative all'incidente stesso;

autovalutazione dell'impatto sui sistemi e sull'erogazione dei servizi di business; o definizione e pianificazione di un piano di rientro. Rientrano in tale fase le attività di preparazione della segnalazione dell'incidente, ove prevista.

R-PY Rev. 1 Regolamento aziendale per la corretta gestione delle violazioni dei dati personali e delle notifiche degli incidenti aventi impatto sui beni



Il **Coordinatore del Gruppo Privacy** o in sua assenza, il Direttore della S.C. Sistemi Informativi avverte tempestivamente il DPO e il suo Team utilizzando gli appositi dati di contatto (posta elettronica e telefono).

Fase 3 – Chiusura dell'incidente

Una volta definite ed avviate le attività di ripristino, il **Coordinatore del Gruppo Privacy** ne dà tempestiva comunicazione al CSIRT Italia (art.3, co. 8 DPCM n. 81/2021), che ha la facoltà di richiedere al soggetto stesso una relazione tecnica dell'incidente riguardante gli aspetti significativi dell'incidente, quali:

- una valutazione delle conseguenze dell'impatto sui beni ICT;
- la descrizione delle azioni di recupero e ripristino intraprese.

A seguito della richiesta il **Coordinatore del Gruppo Privacy** è tenuto a rispondere al CSIRT Italia, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa, entro trenta giorni, ai sensi dell'art. 3, co. 8, del DPCM n. 81/2021.



Dipartimento Tutela della Salute
e Politiche Sanitarie

10 ESEMPI DI INCIDENTI DI SICUREZZA

TIPO DI BREACH	DEFINIZIONE	CRITERI PER LA SEGNALEAZIONE	ESEMPI DI CASI DA SEGNALEARE	ESEMPI DI CASI DA NON SEGNALEARE
DISTRUZIONE	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Dati non recuperabili o provenienti da procedure non ripetibili.	Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente. Incendio di archivio cartaceo delle cartelle cliniche. Distruzione di campioni biologici.	Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia). Rottura di un PC che non contiene dati personali originali. Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura.
PERDITA	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo ed è possibile che terzi possano avere impropriamente accesso al dato.	Dati non recuperabili o provenienti da procedure non ripetibili. Dati la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato.	Smarrimento di chiavetta USB contenente dati originali. Smarrimento di fascicolo cartaceo personale dipendente.	Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa.
MODIFICA	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Modifiche sistematiche su più casi.	Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup. Azione involontaria, o fraudolenta, di un utente che porta alla alterazione di dati sanitari in modo non tracciato e irreversibile.	Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di recovery. Azione involontaria di un utente che porta all'alterazione di dati tracciata e reversibile. Modifica di un documento non ancora validato dal proprio autore.
DIVULGAZIONE NON AUTORIZZATA	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione.	Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet. Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.
ACCESSO NON AUTORIZZATO	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolari ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi. Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico.	Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi. Accesso non autorizzato di un documento non ancora validato dal proprio autore.
INDISPONIBILITA' TEMPORANEA DEL DATO	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup. Cancellazione accidentale dei dati da parte di una persona non autorizzata. Perdita della chiave di decrittografia di dati crittografati in modo sicuro.	Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso.

Un *data breach*, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente).

I casi di *data breach* per le casistiche già descritte si estendono ai documenti cartacei o su supporti analogici.

La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato *data breach*, ma è considerato un normale errore procedurale. Questo poiché chi riceve non può sapere a quale paziente fisico è riferito il testo o il paziente fisico non è danneggiato poiché nessuno riferimento alla sua persona è stato diffuso.

11. REGISTRO DELLE VIOLAZIONI

Il **Coordinatore del Gruppo Privacy**, con il supporto del Responsabile Protezione Dati (RPD), cura l'aggiornamento del registro delle violazioni (Allegato 3), ai sensi dell'art. 33 comma 5 del REGOLAMENTO.

ALLEGATO 1 –

**NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) e NOTIFICA DI
INCIDENTE INFORMATICO**

Sezione A - Dati del soggetto che effettua la segnalazione

Cognome e nome _____

E-mail _____

Recapito telefonico _____

Funzione rivestita _____

Sezione B – Tipologia impatto

Descrizione del bene ICT _____

Dettagli dell'incidente _____

Descrizione della violazione _____

Sezione C - Informazioni in sintesi

Quando si è venuti a conoscenza della violazione _____

Natura della violazione e dell'incidente

☐ Perdita di confidenzialità

☐ Perdita di integrità

☐ Perdita di disponibilità

Causa della violazione

☐ Azione intenzionale interna

☐ Azione accidentale interna

☐ Azione intenzionale esterna

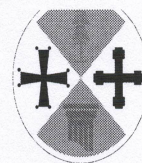
☐ Azione accidentale esterna

☐ Sconosciuta

☐ Note _____

Da inviare per email al seguente indirizzo: privacy@asp.cz.it

Anticipare telefonicamente al Coordinatore del Gruppo Privacy



ALLEGATO 2 – COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali (Regolamento (UE) 679/2016), L'Azienda Sanitaria Provinciale di Catanzaro, titolare del trattamento, con la presente Le comunica l'intervenuta violazione dei Suoi dati personali (data breach), che si è verificata in data _____ alle ore _____
e/o, di cui si è avuta conoscenza in data _____ alle ore _____.

A) Descrizione della natura della violazione

Modalità della violazione dei dati: _____.

Tipo di violazione:

- ☐ Lettura,
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare),
- ☐ Alterazione (i dati sono stati alterati),
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione),
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione).

Dispositivo oggetto di violazione:

- ☐ Computer, ☐ Rete, ☐ Dispositivo mobile, ☐ Strumento di backup, ☐ Documento cartaceo.

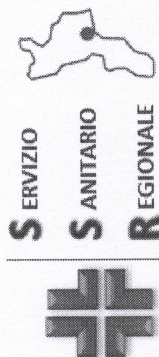
Tipo di dati oggetto di violazione:

- ☐ Dati anagrafici,
- ☐ Dati di accesso e di identificazione (user name, password, altro),
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica,
- ☐ Dati personali idonei a rivelare lo stato di salute,
- ☐ Dati personali idonei a rivelare la vita sessuale,
- ☐ Dati giudiziari,
- ☐ Dati genetici,
- ☐ Dati biometrici,
- ☐ Dati _____
- ☐ Ancora sconosciuti.

B) Descrizione delle probabili conseguenze della violazione di dati personali:

C) Descrizione delle misure tecnologiche e organizzative assunte per porre rimedio alla violazione e se del caso per contenere la violazione dei dati o per attenuarne i possibili effetti negativi:

Per maggiori informazioni relativamente alla violazione in oggetto, si forniscono i seguenti recapiti:
posta elettronica: privacy@asp.cz.it



CA
ZI
EN
DA
SA
NI
TA
RI
A
PR
OV
IN
CIA
LE

CA
TA
NZ
A
RO

ALLEGATO 3 – REGISTRO DELLE VIOLAZIONI

Dipartimento Tutela della Salute
e Politiche Sanitarie[illegible]

A cura del Gruppo Privacy

ALLEGATO 4 Tassonomia degli incidenti

in accordo alla Determina ACN del 3 gennaio 2023 (Allegato A, articolo 3, comma 1)

Identificativo	Categoria	Descrizione
ICP-C-1	Accesso iniziale (<i>Initial exploitation</i>)	Accesso iniziale (<i>Initial access</i>). Il soggetto ha evidenza dell'effettivo accesso non autorizzato all'interno della rete attraverso vettori di infezione, lo sfruttamento di vulnerabilità di risorse esposte pubblicamente o qualsiasi altra tecnica nota.
ICP-C-2	Esecuzione (<i>Execution</i>)	Esecuzione (<i>Execution</i>). Il soggetto ha evidenza dell'effettiva esecuzione non autorizzata di codice o malware all'interno della rete aziendale.
ICP-C-3	Installazione (<i>Establish persistence</i>)	Ottenimento di privilegi di livello superiore (<i>Privilege Escalation</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere permessi di livello superiore su un sistema o una rete.
ICP-C-4		Persistenza (<i>Persistence</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte su un sistema o all'interno della rete, utili ad ottenere persistenza di codice malevolo o a garantire un accesso.
ICP-C-5		Evasione delle difese (<i>Defence Evasion</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, di elusione di politiche e/o sistemi di sicurezza, volte ad evitare il rilevamento durante un tentativo di compromissione.
ICP-C-6		Comando e Controllo (<i>Command and Control</i>). Il soggetto ha evidenza di comunicazioni non autorizzate verso l'esterno della rete.
ICP-C-7	Movimenti laterali (<i>Lateral Movement</i>)	Esplorazione (<i>Discovery</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili a effettuare attività di ricognizione per acquisire conoscenze sul sistema e sulla rete interna.
ICP-C-8		Raccolta di credenziali (<i>Credential Access</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad acquisire, dall'interno della rete, credenziali valide per l'autenticazione alle risorse di rete o ne rinviene copie non autorizzate.
ICP-C-9		Movimenti laterali (<i>Lateral Movement</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad accedere, controllare o eseguire codice tra le risorse interne della rete.
ICP-C-10	Azioni sugli obiettivi (<i>Actions on objectives</i>)	Raccolta (<i>Collection</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a ricercare e/o raccogliere, dall'interno della rete, dati riservati e/o sensibili ovvero ne rilevi la presenza al di fuori dei sistemi autorizzati alla trattazione degli stessi.
ICP-C-11		Esfiltrazione (<i>Exfiltration</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad esfiltrare dati dall'interno della rete verso risorse esterne.
ICP-C-12		Inibizione delle funzioni di risposta (<i>Inhibit Response Function</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a inibire l'intervento delle funzioni di sicurezza, di protezione e di "quality assurance" dei sistemi di controllo industriale predisposte per rispondere a un disservizio o a uno stato anomalo.
ICP-C-13		Compromissione dei processi di controllo (<i>Impair Process Control</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a manipolare, disabilitare o danneggiare i processi di controllo fisico di sistemi di controllo industriale.
ICP-C-14		Disservizio intenzionale (<i>Impact</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a manipolare, degradare, interrompere o distruggere i sistemi, i servizi o i dati. In tale ambito rientrano ad esempio gli eventi di tipo <i>Denial of Service/Distributed Denial of Service</i> che hanno impatto sui beni ICT.