1. Linea guida / Policy per la gestione del "Data Breach" (violazione dei dati personali)

1.1 Premessa

L'art. 24 co. 1 del Regolamento Europeo n. 679/2016 (GDPR) richiede al titolare di "mettere in atto misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR".

L'art. 33 GDPR (Notifica di una violazione dei dati personali all'autorità di controllo) impone al titolare del trattamento di notificare all'autorità di controllo, ed in alcuni casi anche agli interessati, la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di **notifica** all'autorità di controllo scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche; qualora il rischio fosse elevato, oltre alla notifica, il titolare è tenuto a darne **comunicazione** anche all'interessato (**art. 34** - Comunicazione di una violazione dei dati personali all'interessato). Il termine per adempiere alla notifica è appunto di 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio. L'eventuale **ritardo** nella notificazione deve essere giustificato. Il **mancato** rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti **dall'art. 58 GDPR** (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati) e la imposizione di sanzioni amministrative secondo **l'art. 83 GDPR**.

1.2 Violazione di dati

Per "**violazione di dati**" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la

1. Richtlinien / Policy betreffend Vorgehensweise bei einem „Data Breach" (Verletzung personenbezogener Daten)

1.1 Vorausgeschickt

Der **Art. 24 Abs. 1 der EU-Verordnung Nr. 679/2016 (DSGVO)** verlangt vom Verantwortlichen die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um sicherzustellen und um entsprechend auch den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt.

Gemäß **Artikel 33 DSGVO** (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde) muss der Verantwortliche der Aufsichtsbehörde, und in einigen Fällen auch den betroffenen Personen, die Verletzung personenbezogener Daten (**data breach**) binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, melden.

Die **Meldepflicht** an die Aufsichtsbehörde besteht, wenn anzunehmen ist, dass die Verletzung des Schutzes personenbezogener Daten zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt; sollte das Risiko hoch sein, ist der Verantwortliche zusätzlich zur Meldung auch verpflichtet, die betroffene Person zu **benachrichtigen** (**Art. 34** - Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person). Die Frist für die Durchführung der Meldung beträgt, wie erwähnt, 72 Stunden ab dem Zeitpunkt, ab welchem dem Verantwortlichen die Verletzung bekannt wurde, während hingegen die Benachrichtigung der betroffenen Personen unverzüglich zu erfolgen hat. Eine etwaige **Verzögerung** der Meldung ist zu begründen. Bei **Nichteinhaltung** der Meldepflicht kann die Aufsichtsbehörde die ihr zur Verfügung stehenden Korrekturmaßnahmen anwenden, und zwar: die Ausübung der in **Art. 58 DSGVO** vorgesehenen Befugnisse (Abmahnungen, Verwarnungen, Anweisungen, Auferlegung von Beschränkungen der Verarbeitung, Anordnung einer Berichtigung, Widerruf von Zertifizierungen, Aussetzung der Übermittlung von Daten) und die Verhängung von Verwaltungsstrafen nach **Art. 83 DSGVO**.

1.2 Verletzung des Schutzes personenbezogener Daten

Als „**Verletzung des Schutzes personenbezogener Daten**" bezeichnet man eine Sicherheitsverletzung die, unbeabsichtigt oder unrechtmäßig, zur

divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (**Art. 4 co.1 pto.12 GDPR**).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti **dall'art. 5 GDPR** per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza, quindi, comprendere se l'incidente ha impatto sulle informazioni e, infine, se tra le informazioni coinvolte dall'incidente vi sono dati personali.

Si possono distinguere tre tipi di violazioni, eventualmente anche in combinazione:

- Violazione di **riservatezza**, ovvero quando si verifica una divulgazione di dati personali non autorizzato o accidentale;
- Violazione di **riservatezza**, ovvero quando si verifica un accesso a dati personali non autorizzato o accidentale;
- Violazione di **integrità**, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
- Violazione di **disponibilità**, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

1.3 Identificazione dell'incidente di sicurezza

Il Titolare deve strutturare il trattamento dei dati personali avvalendosi di un sistema di conformità e gestione del rischio, che preveda **una procedura per la gestione degli incidenti.**

Il **considerando 85** del GDPR offre utili elementi per determinare i rischi che possono determinare l'obbligo di notifica, in particolare, occorre valutare se la violazione possa causare danni fisici, materiali o immateriali alle persone fisiche:

- perdita del controllo dei dati personali che li riguardano;
- limitazione dei loro diritti;
- discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;

Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von - beziehungsweise zum unbefugten Zugang zu - personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (**Art. 4 Abs. 1, Pkt. 12 DSGVO**).

Die Verletzung des Schutzes personenbezogener Daten ist eine besondere Art von Sicherheitsunfall, durch welchen der Verantwortliche nicht in der Lage ist, die Einhaltung der in **Art. 5 DSGVO** festgelegten Grundsätze für die Verarbeitung personenbezogener Daten zu gewährleisten.

Zunächst muss der Verantwortliche also in der Lage sein, das Sicherheitsunfall zu erkennen, dann zu verstehen, ob der Unfall Auswirkungen auf die Informationen hat und, schließlich, ob die von dem Unfall betroffenen Informationen personenbezogene Daten enthalten.

Es lassen sich drei Arten von Verletzungen unterscheiden, die auch in Kombination vorliegen können:

- Verletzung der **Vertraulichkeit**, d.h. wenn eine Offenlegung von personenbezogenen Daten erfolgt, egal ob dies versehentlich oder unbefugt passiert;
- Verletzung der **Vertraulichkeit**, d.h. wenn ein Zugriff auf personenbezogene Daten erfolgt, egal ob dies versehentlich oder unbefugt passiert;
- Verletzung der **Integrität**, d.h. wenn eine unbefugte oder versehentliche Änderung personenbezogener Daten erfolgt;
- Verletzung der **Verfügbarkeit**, d.h. bei Verlust, bei Unzugänglichkeit oder bei Zerstörung von personenbezogenen Daten, egal ob dies versehentlich oder unbefugt passiert.

1.3 Erkennung des Sicherheitsunfalls

Der Verantwortliche muss die Verarbeitung personenbezogener Daten mit Hilfe eines Systems strukturieren, welches die Konformität und das Risikomanagement verfolgt **und ein Verfahren für die Vorgehensweise bei Unfällen** vorsieht.

Der **Erwägungsgrund 85** der DSGVO stellt nützliche Elemente zur Bestimmung der Risiken bereit, die zur Meldepflicht führen können, und insbesondere ist zu prüfen, ob die Verletzung den natürlichen Personen physische, materielle oder immaterielle Schäden zufügen kann:

- Verlust der Kontrolle über die personenbezogenen Daten, die sie betreffen;
- Einschränkung ihrer Rechte;
- Diskriminierung;
- Identitätsdiebstahl oder -betrug;
- finanzielle Verluste;
- unbefugte Aufhebung der Pseudonymisierung;
- Rufschädigung;

- perdita di riservatezza dei dati personali protetti da segreto professionale;
- o qualsiasi altro danno economico o sociale significativo per la persona interessata.

- Verlust der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegen;
- oder jegliche andere Art von erheblichem wirtschaftlichen oder sozialen Schaden für die betroffene natürliche Person.

L'art. **33 co.2 GDPR** prevede espressamente il dovere per il responsabile del trattamento, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare del trattamento.

Der **Art. 33 Abs. 2 DSGVO** sieht ausdrücklich die Pflicht des Auftragsverarbeiters vor, wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, diese dem Verantwortlichen ohne Verzug zu melden ist.

L'art. **33 co. 5 GDPR**, prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma. Ne discende che le attività di scoperta e di trattamento dell'incidente devono essere: documentate;

- adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi);
- tracciabili;
- replicabili;
- ed essere in grado di fornire evidenza nelle sedi competenti.

Der **Art. 33 Abs. 5 DSGVO** verpflichtet den Verantwortlichen jegliche Verletzung des Schutzes personenbezogener Daten zu dokumentieren, damit die Aufsichtsbehörde die Einhaltung der Norm überprüfen kann. Daraus ergibt sich, dass die Tätigkeiten zur Entdeckung und Behandlung des Unfalls:

- dokumentiert sein müssen;
- angemessen sein müssen (es müssen die Verletzungen, die Umstände, die Folgen und die Gegenmaßnahmen angeführt sein);
- rückverfolgbar sein müssen;
- replizierbar sein müssen;
- und in der Lage sein müssen, den zuständigen Stellen Aufschluss über den Unfall zu geben.

Inoltre, ai fini del decorso delle 72 ore per la notifica, deve essere dimostrabile il momento della scoperta dell'incidente.

Darüber hinaus muss für den Ablauf der 72-stündigen Meldefrist der Zeitpunkt der Entdeckung des Unfalls nachweisbar sein.

Quindi il titolare deve valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati. La rapida identificazione dell'incidente e la tempestività della adozione di contromisure possono consentire di scongiurare/limitare i danni derivanti da una violazione a carico degli interessati.

Daher muss der Verantwortliche das Ausmaß voll alldem im Hinblick auf die Auswirkungen auf personenbezogene Daten und auf die Rechte und die Freiheit der betroffenen Personen bewerten. Die frühzeitige Erkennung des Unfalls und die rechtzeitige Anwendung von Gegenmaßnahmen kann helfen, die Schäden zu Lasten der betroffenen Personen, die durch eine Verletzung entstehen, zu verhindern bzw. einzuschränken.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve comunicare la violazione all'interessato senza ingiustificato ritardo (**art. 34 GDPR**; cfr. anche il **considerando 86**).

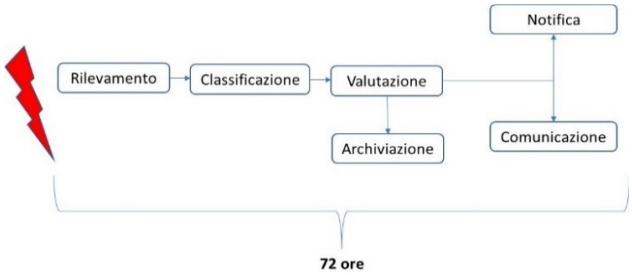
Wenn die Verletzung personenbezogener Daten ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen kann, muss der Verantwortliche die betroffene Person unverzüglich von der Verletzung benachrichtigen (**Art. 34 GDPR**; vgl. auch **Erwägungsgrund 86**).

La notifica e la comunicazione hanno un contenuto pressoché identico (**art. 33 co.3 e art. 34 co.2 GDPR**).

Der Inhalt der Meldung und der Benachrichtigung ist nahezu identisch (**Art. 33 Abs. 3 und 34 Abs. 2 DSGVO**).

La comunicazione va data direttamente e personalmente agli interessati coinvolti dalla violazione; ove ciò comporti sforzi sproporzionati, si procede ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con la medesima efficacia.

Die Benachrichtigung erfolgt unmittelbar und persönlich an die von der Verletzung betroffenen Personen; falls dies mit einem unverhältnismäßigen Aufwand verbunden ist, hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.



1.4 Valutazione del livello di criticità della violazione

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato vanno determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, in base a una valutazione oggettiva (**considerando 76**).

Il WP29 (Data Protection Working Party - Guidelines on Personal data breach notification under Regulation 2016/679) suggerisce ulteriori criteri per permettere una valutazione più accurata (tipo di violazione; natura, sensibilità e volume dei dati personali; facilità di riconoscimento degli interessati; serietà delle conseguenze per le persone fisiche; caratteristiche specifiche delle persone fisiche; quantità di persone fisiche coinvolte; caratteristiche specifiche del titolare).

1.5 Procedura di identificazione e gestione degli incidenti

La tempestività nella notifica può essere assicurata se preesiste un sistema di comunicazione interno adeguato (sistema di report dell'incidente; ricognizione adeguata dell'organizzazione del titolare; valutazioni di impatto sui dati personali (DPIA); ecc.).

Infine, è possibile mostrare la stessa documentazione delle violazioni, che la norma prescrive di conservare (anche per quelle che non determinano obbligo di notifica), solo se è stato strutturato un sistema di gestione degli incidenti.

2. Processo di gestione degli incidenti di sicurezza

2.1 Premessa

Il trattamento degli incidenti di sicurezza presuppone l'esistenza di un sistema di sicurezza delle informazioni che offra tutti gli strumenti necessari:

- La scoperta dell'incidente presuppone un sistema di monitoraggio che a sua volta presuppone l'organizzazione della sicurezza all'interno della Casa di Riposo (definizione degli obiettivi, compiti e responsabilità, individuazione e definizione dei rischi, individuazione dei rimedi).

1.4 Bewertung des Grades der Ernsthaftigkeit der Verletzung

Die Eintrittswahrscheinlichkeit und die Schwere/ Ernsthaftigkeit des Risikos für die Rechte und Freiheiten der betroffenen Person sind in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu bestimmen, wobei dies aufgrund einer objektiven Bewertung zu erfolgen hat (**Erwägungsgrund 76**).

Die Gruppe WP29 (Data Protection Working Party - Guidelines on Personal data breach notification under Regulation 2016/679) schlägt zusätzliche Kriterien vor, um eine genauere Bewertung zu ermöglichen (Art der Verletzung; Art, Sensibilität und Umfang der personenbezogenen Daten; Identifizierbarkeit der betroffenen Personen; Schwere/Ernsthaftigkeit der Folgen für die betroffenen Personen; besondere Eigenschaften der betroffenen Personen; Anzahl der betroffenen Personen; besondere Eigenschaften des Verantwortlichen).

1.5 Verfahren zur Erkennung der Unfälle und über die Vorgehensweise

Die Rechtzeitigkeit der Meldung kann gewährleistet werden, wenn ein angemessenes internes Kommunikationssystem vorhanden ist (Unfallmeldesystem mittels Reports; angemessene Aufklärung der Organisation des Verantwortlichen; Datenschutz-Folgenabschätzungen (DSFA); usw.).

Zudem ist es nur dann möglich, wie von der Norm vorgesehen, die Dokumentation von Verletzungen vorzuweisen (auch für jene, für die sich keine Meldepflicht ergibt), wenn ein System für die Vorgehensweise bei Unfällen eingerichtet worden ist.

2. Verfahren für die Vorgehensweise bei Sicherheitsunfällen

2.1 Vorausgeschickt

Die Behandlung von Sicherheitsunfällen erfordert das Vorhandensein eines Sicherheitssystems für die Informationen, welches alle notwendigen „Werkzeuge" bereitstellt:

- Die Feststellung des Unfalls setzt ein Überwachungssystem voraus, das wiederum die Organisation der Sicherheit innerhalb des Seniorenwohnheimes voraussetzt (Festlegung der Ziele, der Aufgaben und der Verantwortlichkeiten, Erhebung und Beschreibung der Risiken, Erhebung der Gegenmaßnahmen).

- La valutazione dell'incidente presuppone la definizione dei criteri di valutazione, la formazione del personale incaricato, la predisposizione di procedure.
- La tempestività nella notifica può essere assicurata se preesiste un sistema di comunicazione interno adeguato e tutti coloro che operano per il titolare abbiano ricevuto adeguate istruzioni.

- Devono essere disponibili le informazioni necessarie, aspetto che richiede un sistema di report dell'incidente, una ricognizione adeguata dell'organizzazione del titolare, e valutazioni di impatto sui dati personali (DPIA).

- Deve essere strutturato un sistema di gestione degli incidenti, anche per conservare la documentazione delle violazioni.

Una corretta gestione delle problematiche di data breach deve anche basarsi su una serie di presupposti organizzativi. In particolare:

- tutti coloro che operano per il titolare devono essere allineati su cosa sia un incidente di sicurezza.
- tutti coloro che operano per il titolare devono essere allineati sul fatto che gli incidenti di sicurezza, una volta accertati, devono essere gestiti dal c.d. Team Privacy; il Team Privacy è costituito da un gruppo di lavoro interno alla Casa di riposo formato dai seguenti membri:

- Direttore
- Presidente
- Tecnico EDP

Al bisogno, oppure in caso di opportunità, su iniziativa del direttore, i citati membri possono essere sostituiti, rispettivamente integrati, con altri collaboratori della Casa di Riposo. Il Team Privacy coinvolge anche il DPO, Dott. Pietro Lanzetta.

- Il Team Privacy opera sotto la responsabilità del Direttore (Responsabile del Trattamento della Casa di Riposo
- In qualunque punto del processo, laddove non ci sia risposta sollecita da parte di utenti e funzioni interne o di Responsabili esterni del trattamento, sarà compito del Responsabile sopra indicato coinvolgere il Titolare del Trattamento e il DPO.

Eventuali incidenti, che fossero riconducibili esclusivamente a prestazioni EDP - prestazioni appunto rese presso quest'ultimo -, saranno gestiti

- Die Bewertung des Unfalls setzt die Festlegung der Bewertungskriterien, die Schulung des beauftragten Personals, die Bereitstellung von Verfahren voraus.
- Die Rechtzeitigkeit der Meldung kann gewährleistet werden, wenn ein angemessenes internes Kommunikationssystem vorhanden ist und alle Personen, die für den Verantwortlichen tätig sind, entsprechende Anweisungen erhalten haben.
- Die erforderlichen Informationen müssen verfügbar sein, was wiederum ein Unfallmeldesystem, eine angemessene Erhebung der Organisation des Verantwortlichen, und Datenschutz-Folgenabschätzungen (DSFA) erfordert.
- Es muss ein Verfahren für die Vorgehensweise bei Unfällen eingerichtet sein, auch um die Dokumentation der Verletzungen aufzubewahren.

Eine korrekte Vorgehensweise im Fall von data breach-Problematiken muss zudem auf einer Reihe von organisatorischen Voraussetzungen aufbauen. Insbesondere:

- müssen alle, die für den Verantwortlichen tätig sind, darüber in Kenntnis sein, was ein Sicherheitsunfall ist.
- müssen alle, die für den Verantwortlichen tätig sind, darüber in Kenntnis sein, dass Sicherheitsunfälle, sobald sie festgestellt werden, vom sog. Privacy-Team behandelt werden müssen; das Privacy-Team ist eine interne Arbeitsgruppe des Seniorenwohnheimes bestehend aus den folgenden Mitgliedern:

- Direktor
- Präsident
- EDV-Techniker

Bei Bedarf, oder soweit opportun, können die vorgenannten Mitglieder, auf Initiative des Direktors, durch andere Mitarbeiter ersetzt bzw. mit anderen Mitarbeitern des Seniorenheimes ergänzt werden. Das Privacy-Team bezieht auch den DPO, Dr. Pietro Lanzetta ein.

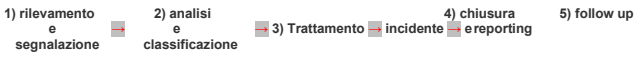
- Das Privacy-Team arbeitet unter der Verantwortung des Direktors
- Falls es keine unmittelbare Rückmeldung seitens der Nutzer und der internen Stellen oder seitens externer Auftragsverarbeiter geben sollte, obliegt es dem obgenannten Auftragsverarbeiter, zu jedem Zeitpunkt des Verfahrens, den Verantwortlichen und den DPO miteinzubeziehen.

Etwaige Unfälle, die ausschließlich auf EDV-Dienstleistungen zurückzuführen sind, die eben im genannten Verband erbracht werden -, werden im

nell'ambito del processo di gestione degli incidenti di sicurezza del Consorzio stesso; in questi casi, tuttavia, tutti coloro che operano per il titolare della Casa di riposo sono comunque tenuti ad utilizzare il canale di helpdesk "IT Security & Data Breach", istituito dal Consorzio, per segnalare tempestivamente e proattivamente eventuali eventi di sicurezza presunti oppure accertati.

2.2 Fasi della procedura

Il processo è suddiviso in fasi come indicato nello schema che segue:



Rilevamento e segnalazione

Questa fase ha la principale finalità di intercettare ed identificare tutti i possibili eventi che possano essere correlati ad un potenziale incidente. La rilevazione e segnalazione è riconducibile a due fonti:

a) Rilevazione Interna: il personale della Casa di Riposo, che opera quindi per il titolare, può identificare:
b)

- eventi di sicurezza sui sistemi o componenti di sistema gestiti internamente;
- eventi di sicurezza relativi ai sistemi eventualmente gestiti da responsabili esterni del trattamento;
- possibili eventi di sicurezza per altri servizi gestiti da altri fornitori.

b) Rilevazione Esterna: eventuali fornitori esterni, a prescindere che siano stati o meno nominati responsabili esterni del trattamento, che identificano eventi di sicurezza.
Le segnalazioni possono essere generate automaticamente dai sistemi mediante alert o manualmente.
1) Segnalazione automatica
La casa di Riposo dispone di un sistema di monitoraggio automatico che visualizza e controlla gli eventi rilevanti per la sicurezza. (Trend Micro Officescan Antivirus - Punti di protezione: Endpoint fisici, Endpoint virtuali (componenti aggiuntivi), PC e server Windows)

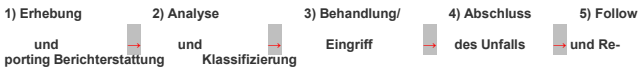
Ove si tratti effettivamente di un evento di sicurezza la segnalazione acquisirà la tipologia di "incidente".

2) Segnalazione manuale
Segnalazioni di eventi di sicurezza possono sorgere all'interno della Casa di Riposo, anche da parte di funzioni interne o di partner/fornitori esterni con i quali la stessa collabora. Tali segnalazioni vengono analizzate e filtrate dal Tecnico EDP, che ricerca/raccoglie anche eventuali altri eventi collegati o riconducibili all'evento di sicurezza.

Rahmen des Verfahrens für die Vorgehensweise bei Sicherheitsunfällen des Seniorenwohnheimes verwaltet; in diesen Fällen sind jedenfalls alle, die für den Verantwortlichen der tätig sind, weiterhin verpflichtet den vom Gemeindenverband eingerichteten Helpdesk-Kanal "IT Security & Data Breach" zu nutzen, um vermutete oder festgestellte Sicherheitsvorfälle unverzüglich und proaktiv zu melden.

2.2 Phasen des Verfahrens

Das Verfahren ist in Phasen unterteilt wie aus dem folgenden Schema ersichtlich:



Erhebung und Berichterstattung

Diese Phase hat in erster Linie den Zweck, alle möglichen Vorfälle, die mit einem möglichen Unfall zusammenhängen können, festzustellen und zu identifizieren. Die Erhebung und Berichterstattung kann in zweierlei Form erfolgen:
a) Interne Erhebung: das Personal des Seniorenwohnheimes welches für den Verantwortlichen tätig ist, kann Folgendes feststellen:

- Sicherheitsvorfälle betreffend Systeme oder Teile von Systemen, die intern verwaltet werden;
- Sicherheitsvorfälle in Bezug auf Systeme, die eventuell von externen Auftragsverarbeitern verwaltet werden;
- mögliche Sicherheitsvorfälle betreffend andere Dienste, die von anderen Lieferanten verwaltet werden.

b) Externe Erhebung: durch etwaige externe Lieferanten, unabhängig davon, ob sie als externe Auftragsverarbeiter ernannt worden sind oder nicht, die Sicherheitsvorfälle feststellen.
Die Berichte können von den Systemen automatisch durch Alerts oder manuell/von Hand erzeugt werden.

1) Automatische Berichterstattung
Das Seniorenwohnheim verfügt über ein automatisches Überwachungssystem, das die sicherheitsrelevanten Vorfälle anzeigt und kontrolliert. (Trend Micro Officescan Antivirus – Schutzbereiche: Physische Endpunkte, Virtualisierte Endpunkte (Add-on), Windows-PCs und Server)

Soweit es sich tatsächlich um einen Sicherheitsunfall handelt wird der gemeldete Vorfall als „Unfall" behandelt.

2) Manuelle Berichterstattung
Berichterstattungen über Sicherheitsvorfälle können ihren Ursprung intern haben, also von internen Dienststellen des Seniorenwohnheimes stammen, oder von externen Partnern/Lieferanten, mit denen diese zusammenarbeiten, vorgebracht werden. Diese Berichte werden vom EDV-Techniker analysiert und gefiltert, und diese sucht/sammelt zudem auch nach etwaigen anderen Vorfällen, die mit dem gemel-

segnalato. Qualora dovesse risultare che la segnalazione sia effettivamente riconducibile a un evento di sicurezza, essa acquisirà, anche in questo caso, tipologia di “Incidente”.

Dai punti 1) e 2) consegue, che tutte le segnalazioni, interne o esterne che siano, vengono raccolte ed analizzate preliminarmente dal Tecnico EDP per una prima analisi e per filtrare quelle ritenute non significative. Le restanti sono da inviare al DPO, Dott. Pietro Lanzetta per la successiva gestione. Le informazioni alla valutazione dell’incidente devono necessariamente comprendere:

- gli asset impattati sia in numero che in tipologia;
- la criticità, la classificazione del processo di gestione del rischio IT, degli asset coinvolti;
- i processi, i servizi e, se del caso, la clientela impattata dall’evento;
- eventuali danni prodotti dall’evento (es. malfunzionamenti, blocchi o degradi di servizi, corruzione di dati, fughe di informazioni, etc);
- in caso di attacco da Internet, sorgenti (es. indirizzi IP), estensione e modalità di attacco;
- altre segnalazioni/allarmi correlati all’evento in esame;
- modalità di propagazione/evoluzione dell’evento;
- altre informazioni ritenute utili.

Queste informazioni consentono la classificazione dell’evento e di attivare tutte le misure di contrasto e contenimento.

A cura della ripartizione CED/EDP gli eventi di sicurezza rilevati rispettivamente segnalati come esposto nei paragrafi che precedono, vengono annotati progressivamente in un **registro degli incidenti di sicurezza**, che rappresenta quindi la sintesi cronologica degli eventi verificatisi nel tempo; il tutto con la specificazione, in relazione ad ogni singolo evento, dei relativi esiti (archiviazione oppure notifica).

Nel caso di qualificazione, anche da parte del DPO, Dott. Pietro Lanzetta, dell’evento quale “evento di sicurezza” comportante un incidente, viene convocato il Team Privacy per la successiva classificazione di dettaglio. In ogni caso, la competente ripartizione della Casa di Riposo potrà già iniziare subito a intraprendere le azioni opportune per la gestione e la risoluzione dell’incidente.

deten Sicherheitsvorfall in Verbindung stehen oder auf diesen rückführbar sein könnten. Sollte sich aus der Berichterstattung herausstellen, dass es sich tatsächlich um einen Sicherheitsvorfall handelt, wird der gemeldete Vorfall, auch hier, als „Unfall“ behandelt.
Aus den Punkten 1) und 2) ergibt sich, dass alle Berichterstattungen, ob intern oder extern, vorab vom EDV-Techniker gesammelt und analysiert werden, um eine erste Auswertung durchzuführen, sowie um diejenigen herauszufiltern, die als unbedeutend angesehen werden können. Die restlichen Berichte sind an den DPO, Dr. Pietro Lanzetta für die darauffolgende Handhabung zu übermitteln. Die Informationen für die Beurteilung des Unfalls müssen unbedingt Folgendes beinhalten:

- die betroffenen Bereiche, sowohl mengenmäßig als auch in Bezug auf deren Typologie;
- die Klassifizierung des IT-Risikomanagement-Prozesses, und die Angabe darüber, wie kritisch die betroffenen Bereiche sind;
- die von dem Vorfall betroffenen Prozesse, Dienstleistungen und, falls zutreffend, die betroffenen Kunden;
- etwaige durch den Vorfall verursachte Schäden (z.B. Fehlfunktionen, Blockierungen oder Beeinträchtigungen von Diensten, Beschädigung von Daten, Verlust von Informationen, usw.);
- im Falle eines Angriffs aus dem Internet, Quellen (z.B. IP-Adressen), den Umfang und die Art des Angriffs;
- andere Berichterstattungen/Alarmmeldungen, die im Zusammenhang mit dem zu prüfenden Vorfall stehen;
- Art der Ausbreitung/Entwicklung des Ereignisses;
- andere Informationen, die als nützlich erachtet werden.

Diese Informationen ermöglichen es die Klassifizierung des Vorfalles vorzunehmen und alle Gegenmaßnahmen sowie Maßnahmen zur Eindämmung einzuleiten.

Die EDV-Abteilung betreut die fortlaufende Aufzeichnung der, wie in den vorstehenden Absätzen beschrieben, erkannten bzw. gemeldeten Sicherheitsvorfälle in einem **Verzeichnis der Sicherheitsvorfälle**, welches somit die chronologische Zusammenfassung der im Laufe der Zeit eingetretenen Vorfälle darlegt; dies alles unter spezifischer Angabe, in Bezug auf jeden einzelnen Vorfall, des entsprechenden Ausgangs (Archivierung oder Benachrichtigung).

Falls auch der DPO, Dr. Pietro Lanzetta, den Vorfall als "Sicherheitsereignis" mit Unfallfolge klassifizieren sollte, trifft sich das Privacy-Team, um die darauf folgende Detaileinstufung vorzunehmen. In jedem Fall muss die zuständige Dienststelle des Seniorenwohnheimes umgehend damit beginnen, geeignete Maßnahmen zur Handhabung und zur Lösung des Unfalls zu ergreifen.

Analisi e classificazione

L'analisi e la classificazione di dettaglio degli eventi di sicurezza ad opera del Team Privacy è volta a categorizzare l'incidente in modo più granulare, sulla base della gravità (in incidente operativo, incidente di sicurezza informatica, incidente grave, crisi) individuando così le attività necessarie per il suo trattamento.

Il Team Privacy segnala tempestivamente l'incidente al titolare del trattamento e al DPO.

Sulla base delle informazioni fornite riguardanti l'entità dell'incidente, sarà cura del titolare del Trattamento col supporto del DPO provvedere alla valutazione d'impatto dell'incidente sul proprio contesto operativo e prendere una decisione in merito alla necessità di procedere alla "Notifica" e alla "Comunicazione".

Trattamento

La fase di trattamento del processo di gestione degli incidenti ha la principale finalità di attivare tutte le azioni necessarie a gestire l'evento segnalato.

Essa consiste nell'attuazione di tutte le misure di contenimento e riduzione degli impatti da porre in essere.

Nel caso di incidente di sicurezza dovrà essere mantenuto un opportuno aggiornamento mediante canali tempestivi tra il la Ripartizione CED/EDP, il Team Privacy, il titolare del trattamento e il DPO, ai fini di consentire agli stessi visibilità costante sullo stato di avanzamento della gestione e risoluzione dell'incidente e di rispettare le tempistiche stringenti previste dal Regolamento.

In caso di necessità, il titolare del trattamento procederà, nel rispetto dei tempi richiesti, ad attivare la notifica all'Autorità di controllo competente con il supporto del DPO.

Analoga azione dovrà essere fatta, sempre a cura del titolare del Trattamento, nel caso in cui si evidenzi la necessità di comunicazione dell'incidente al/ai soggetti interessati.

Formalizzazione del procedimento

Degli incontri del Team Privacy viene redatto un conciso verbale, al quale potrà essere anche allegata la corrispondenza che il citato gruppo di lavoro progressivamente formalizza in relazione agli incidenti oggetto di analisi e di trattamento, sia essa rivolta verso destinatari interni oppure anche verso l'esterno.

Analyse und Klassifizierung

Die detaillierte Analyse und Klassifizierung der Sicherheitsvorfälle durch das Privacy-Team zielt darauf ab, den Unfall auf eine detailliertere Art und Weise einzustufen und zwar ausgehend von dessen Schwere/Ernsthaftigkeit (Betriebsunfall, Computer-sicherheitsunfall, schwerer Unfall, Krise), wodurch die erforderlichen Eingriffe für dessen Behandlung erhoben werden.

Das Privacy-Team zeigt den Unfall umgehend gegenüber dem Verantwortlichen der Datenverarbeitung und dem DPO auf.

Auf der Grundlage der übermittelten Informationen betreffend das Ausmaß des Unfalls, obliegt es dann dem Verantwortlichen, mit der Unterstützung des DPO's, die Auswirkungen des Unfalls auf die Operativität zu bewerten und eine Entscheidung über die Notwendigkeit der „Meldung" und der „Benachrichtigung" zu treffen.

Behandlung/Eingriff

Die Phase der Behandlung/des Eingriffs hat im Verfahren über die Vorgehensweise bei Unfällen in erster Linie den Zweck, alle Maßnahmen in die Wege zu leiten, die zur Bewältigung des gemeldeten Vorfalls erforderlich sind.

Diese Phase besteht in der Umsetzung aller Maßnahmen, die zur Eindämmung und Begrenzung der Auswirkungen beitragen.

Im Falle eines Sicherheitsunfalls muss auf zeitnahem Wege ein angemessener Informationsaustausch zwischen der EDV-Abteilung, dem Privacy-Team, dem Verantwortlichen der Datenverarbeitung und dem DPO bestehen, um allen ständig Überblick über den Fortschritt in der Handhabung und Lösung des Unfalls zu gewährleisten und um die in der Verordnung vorgesehenen zeitlich knappen Fristen einzuhalten.

Falls erforderlich, wird der Verantwortliche der Datenverarbeitung mit der Unterstützung des DPO's innerhalb der vorgeschriebenen Fristen die Meldung an die zuständige Aufsichtsbehörde vornehmen.

Die gleiche Vorgehensweise muss der Verantwortliche der Datenverarbeitung einhalten, falls die Notwendigkeit entsteht, die betroffene/n Person/en über den Unfall zu benachrichtigen.

Formalisierung des Verfahrens

Es wird ein kurzes Sitzungsprotokoll über die Treffen des Privacy-Teams erstellt, dem auch die Korrespondenz beigefügt werden kann, welche die vorgenannte Arbeitsgruppe in Bezug auf die zu analysierenden und behandelnden Unfälle fortlaufend übermittelt, sei es an interne Empfänger oder auch nach außen hin.

Chiusura incidente

Nel momento in cui l'evento viene risolto, la funzione ripartizione CED/EDP effettua la verifica di quanto risolto e procede all'aggiornamento del sistema di gestione degli incidenti elaborando una relazione tecnica sull'incidente. Questa relazione tecnica espone tutti i passi compiuti dal rilevamento dell'evento fino alla chiusura dell'incidente (cioè: cause che hanno determinato l'evento/incidente; gli interventi e le eventuali contromisure adottate, anche per evitare che l'incidente si ripeta in futuro; le informazioni raccolte in fase di classificazione e analisi e, per quanto riguarda gli incidenti, le azioni di contrasto, contenimento e ripristino adottate, le vulnerabilità/minacce riscontrare, con indicazione della relativa gravità). La relazione va predisposta anche per quelle segnalazioni, che non hanno determinato un obbligo di notifica o di comunicazione.

Follow up e Reporting

Il Team Privacy, ad avvenuta chiusura dell'incidente, esamina la relazione tecnica di cui al punto precedente e informa quindi il titolare del trattamento, oltre al DPO, in forma di conciso verbale conclusivo, delle cause che hanno determinato l'incidente e degli interventi che sono stati identificati/implementati, affinché lo stesso non si ripeta.

Abschluss des Unfalls

Wenn der Vorfall behoben ist, überprüft die EDV-Abteilung die vorgenommenen Eingriffe und aktualisiert das Verfahren über die Vorgehensweise bei Unfällen, indem sie einen technischen Bericht über den Unfall erstellt. Dieser technische Bericht beschreibt alle Maßnahmen, die von der Erkennung des Ereignisses bis zur Schließung des Unfalls ergriffen wurden (d.h.: die Ursachen des Vorfalles/Unfalles; die getätigten Eingriffe und die eventuell getroffenen Gegenmaßnahmen, auch um zu verhindern, dass sich der Unfall in Zukunft wiederholt; die während der Klassifizierungs- und Analysephase gesammelten Informationen und, was die Unfälle betrifft, die Maßnahmen die zu ihrer Bekämpfung, Eindämmung und zur Wiederherstellung umgesetzt worden sind, die aufgetretenen Schwachstellen/ Bedrohungen, mit Angabe der entsprechenden Gefährlichkeit). Der Bericht ist auch für jene Situationen zu erstellen, die nicht zu einer Melde- oder Berichtigungspflicht geführt haben.

Follow up und Reporting

Das Privacy-Team sichtet nach Abschluss des Unfalls den im vorherigen Punkt genannten technischen Bericht und informiert dann den Verantwortlichen und den DPO, in der Form eines prägnanten Abschlussberichts, über die Ursachen, die zu dem Unfall geführt haben, und über die identifizierten/umgesetzten Maßnahmen, damit sich der Unfall nicht wiederholt.