Public

PROTEZIONE DI BT

Standard relativo alla Classificazione delle Informazioni e Trattamento dei Dati per le Terze Parti

Standard: 4.0 **Proprietario:** BT Security

Nel presente standard vengono indicati i controlli di sicurezza base validi per le Terze parti che potranno accedere, archiviare o elaborare le Informazioni BT.

Si applica a tutte le Terze parti che lavorano per o per conto del Gruppo BT, compresi Openreach, EE e PlusNet. Per semplicità, nel presente documento ci limiteremo all'uso della sigla 'BT'.

Introduzione

BT classifica i dati e le informazioni in categorie diverse in base al danno che potrebbe derivare da una relativa perdita o dalla divulgazione non autorizzata. Al momento della creazione, tutti i dati e le informazioni vengono valutati per determinarne la categoria di classificazione appropriata.

I dati e le informazioni devono essere conservati per un periodo di tempo adeguato nel rispetto di requisiti legali, normativi e commerciali, al termine del quale dovranno essere eliminati in sicurezza. Tutte le apparecchiature su cui vengono memorizzati i dati dovranno essere ugualmente smaltite al termine della loro vita operativa. Lo smaltimento delle apparecchiature deve essere svolto nel modo più rispettoso dell'ambiente possibile.

Il presente standard definisce i requisiti per la classificazione delle informazioni, l'etichettatura, la gestione/il trattamento, la conservazione e l'eliminazione dei dati e degli asset informativi di BT.

Definizione dei termini:

Termine	Spiegazione
deve/devono	Questa espressione, o i termini 'RICHIESTO/NECESSARIO' o 'DOVRÀ', indica un requisito assoluto
non deve/non devono	Questa espressione, o l'espressione 'NON DOVRÀ', indica un divieto assoluto
può/potrebbe/possono/potrebbero	Questo termine, o l'aggettivo 'OPZIONALE', indica che l'indicazione fornita è effettivamente opzionale
dovrebbe/dovrebbero	Questo termine, o l'aggettivo 'CONSIGLIATO', indica che sussiste un valido motivo in determinate circostanze per ignorare una determinata indicazione, ma le implicazioni verranno pienamente comprese e attentamente valutate prima di scegliere un'opzione diversa.
non dovrebbe/non dovrebbero	Questa espressione, o l'espressione "NON CONSIGLIATO", indica che verrà fatto ogni ragionevole sforzo per soddisfare i requisiti di una misura di controllo, ma non sempre sarà possibile evitare l'azione descritta in tutti i casi. Nei casi in cui non sia possibile soddisfare un controllo, le implicazioni verranno valutate e pienamente comprese.
BT	Questo termine indicherà il Gruppo BT, compresi Openreach, EE e Plusnet. Per semplicità, nel presente documento ci limiteremo all'uso della sigla 'BT'.

Ambito di applicazione

Il presente standard si applica a tutti i dati e alle informazioni di BT, in qualsivoglia formato. Sono compresi tutti i documenti cartacei ed elettronici, multimediali (foto, video, WebEx, ecc.), orali (conversazioni telefoniche/segreteria telefonica) e i dati e le informazioni conservati in sistemi, applicazioni o apparecchiature in grado di memorizzare, elaborare o trasmettere dati. L'ambito di applicazione del presente standard copre la classificazione delle informazioni, l'etichettatura, la gestione/il trattamento, la conservazione e l'eliminazione.

Cosa include il presente documento?

1. Introduzione alla Classificazione delle Informazioni.

Non tutte le informazioni conservate o trattate da una terza parte per BT avranno lo stesso valore o lo stesso grado di sensibilità. Spetterà a BT classificare le informazioni che rientrano nell'ambito del servizio prestato a garanzia che venga applicato un livello di protezione idoneo alle informazioni, e che le informazioni vengano gestite in modo efficace e sicuro.

Le informazioni possono essere classificate secondo uno schema sviluppato da BT che comprende quattro diverse categorie:

- Public (Informazioni pubbliche)
- Internal (Informazioni per uso interno)
- Confidential (Informazioni riservate)
- Highly Confidential (Informazioni strettamente riservate)

I soggetti che non sono stati informati in merito alla classificazione delle informazioni che stanno gestendo sono pregati di contattare il proprio Stakeholder BT o il Procurement Buyer.

2. Livelli di Classificazione di BT.

Public

Informazioni specificatamente approvate per la pubblicazione generale. Le informazioni che rientrano in questa classe non sono soggette e requisiti di trattamento particolari

Esempi: Dettagli relativi ai nostri prodotti e servizi, informazioni pubblicate su un sito web esterno a BT, comunicati stampa, white paper, materiale pubblicitario.

Internal

Informazioni la cui divulgazione non autorizzata, in particolare al di fuori di BT, sarebbe inappropriata. La pubblicazione di dette informazioni non gioverebbe agli interessi di BT. Queste informazioni possono essere limitate ad alcuni gruppi o funzioni specifiche all'interno dell'azienda.

NB: Se una Terza parte accede a dette informazioni o è incaricata della relativa conservazione, le informazioni rientrano nella classe "Confidential"

Esempi: Informazioni relative all'azienda o ai dipendenti su intranet, gran parte delle politiche, degli standard, dei processi e delle procedure di BT, gran parte della documentazione di progetto e dei verbali di riunione

Confidential

La divulgazione non autorizzata di queste informazioni, seppure all'interno dell'organizzazione, potrebbe causare un danno notevole agli interessi di BT. L'accesso a tali informazioni, e la relativa condivisione, è limitato esclusivamente a soggetti autorizzati per necessità specifiche che rientrano nell'ambito del loro lavoro. I danni potrebbero comportare una perdita finanziaria, perdita di redditività o di opportunità, imbarazzo o perdita di reputazione, oppure portare a una sanzione legale o amministrativa nei confronti di BT. I dati personali, le informazioni sulle carte di pagamento o la proprietà intellettuale sono classificati come 'Confidential'.
La informazioni riservate sono soggette a requisiti di gestione specifici che devono essere rispettati.

Esempi: Dati personali relativi ai nostri dipendenti, a terzi o ai clienti (inclusi i relativi pagamenti finanziari), come: Contratti dei dipendenti, dati sulle performance, sondaggi CARE, identificativi di servizio personali (ID servizio, identificativo a banda larga, identificativo PSTN). Alcuni documenti di progetto relativi a infrastrutture o progetti di importanza critica, diagrammi di rete, contratti di fornitura di terzi. Dati di registro di sistema, dati relativi alle vendite e alle attività di marketing (variazioni di tariffe prima del lancio prodotto, performance finanziarie prima della pubblicazione sui mercati), business plan locali, dati relativi ai rischi, dati sulle chiamate e informazioni riservate

Highly Confidential

La divulgazione di queste informazioni ha un'influenza presumibilmente negativa sul raggiungimento degli obiettivi aziendali principali. Queste informazioni sono straordinariamente sensibili poiché, in caso di fuga, possono creare un danno grave. L'accesso alle informazioni strettamente riservate è limitato a una cerchia ristretta di persone. Ai soggetti non autorizzati l'accesso deve essere assolutamente vietato. I requisiti di gestione sono molto più severi rispetto a quelli relativi alle informazioni riservate. Per via dei danni molto gravi che potrebbero verificarsi, questa classificazione è molto restrittiva. A tutti i soggetti che trattano questo tipo di informazioni potrebbe essere richiesta la sottoscrizione di un accordo di riservatezza (NDA) o un 'Insider list'.

Esempi: Password di computer, registro dei rischi per la sicurezza, alcuni dati personali sensibili come le informazioni sulle carte di pagamento, il numero di previdenza sociale e i dati riportati sui passaporti. Informazioni sensibili sulle risorse umane che potrebbero alienare un numero significativo di dipendenti, business plan strategici, strategia competitiva, nuovi prodotti strategici e nuove politiche di marketing, valutazioni su concorrenti, partner o appaltatori molto sensibili, uso di Internet, numero di account clienti, relazioni degli audit o dati contenenti dettagli relativi a gravi difetti/vulnerabilità nelle pratiche o nei processi di BT, informazioni che potrebbero influire sul valore delle nostre azioni, compresi i verbali di consiglio, informazioni sensibili relative ai prezzi, informazioni concernenti fusioni e acquisizioni, eventi relativi alla sicurezza, chiavi di crittografia, documentazione inerente alla strategia aziendale, business plan

3. Requisiti di Gestione e Trattamento.

Nota: Se non specificatamente inclusi, non sussistono requisiti di gestione particolari associati alle informazioni classificate come 'Public'.

3.1 Gestione di dati veicolati oralmente o in formato multimediale.

Riferimento	Cosa si desidera fare con queste informazioni?	Classificazione	Requisiti di gestione
HSMS10	Voglio pubblicare le informazioni sui social media/network	Public	I dati possono essere pubblicati in qualsiasi gruppo, ad esempio Splash o Yammer. È vietato lasciare il proprio contributo su siti o postare dichiarazioni online che potrebbero essere ragionevolmente attribuite alla visione di BT.
		Internal/Confidential	Non consentito.
		Highly Confidential	Non consentito
HSMS20	Voglio parlare con qualcuno usando il servizio di messaggistica istantanea interno, ad esempio Microsoft Lync	Internal/Confidential	È possibile usare i servizi messi a disposizione di BT/interni Live Meeting, WebEx, Webjoin e Skype for Business. Prima di affrontare qualsiasi tipo di argomento, accertarsi di aver selezionato i soggetti corretti. Non divulgare le seguenti informazioni: · **Qualsivoglia informazioni sulle carte di pagamento.** · **Dati personali.** · **Coordinate bancarie.** · **PIN o altre password.**
		Highly Confidential	Non consentito.
HSM30	Voglio parlare con qualcuno tramite la live chat esterna. Ad esempio, su un sito di assistenza di un vendor come Cisco	Public	Le conversazioni devono essere limitate alle "Informazioni Public" che sono liberamente disponibili sul nostro sito web BT esterno
		Internal/Confidential	È consentito esclusivamente previa verifica dell'identità della persona o delle persone con cui si sta chattando. La divulgazione delle informazioni riservate relative a determinati soggetti deve avvenire nel rispetto del principio della necessità (*Need-to-Know*), fermo restando che le informazioni indicate di seguito non devono mai essere diffuse: · **Qualsivoglia informazioni sulle**

			carte di pagamento. · **Dati personali.** · **Coordinate bancarie.** · **PIN o altre password.**
		Highly Confidential	Non consentito.
HSM40	Voglio parlare con qualcuno faccia a faccia o al telefono	Internal/Confidential	Prima di discutere di eventuali informazioni riservate è necessario verificare l'identità della persona con cui si sta parlando e la divulgazione è rigorosamente disciplinata dal principio della necessità (comprese le conversazioni in negozio e tramite call centre) Se applicabile, prima di avviare la conversazione si deve sottoscrivere un NDA. Assicurarsi che nessun'altra persona senza "diritto di sapere" in base al principio della necessità possa ascoltare la conversazione. Mai lasciare queste informazioni su sistemi di segreteria telefonica.
		Highly Confidential	Come le informazioni "Confidential". Fare in modo che le informazioni "Highly Confidential" siano limitate.
HSM50	Voglio inviare un messaggio a tutte le parti (interne ed esterne)	Public	Il contenuto dei messaggi deve essere limitato alle "Informazioni pubbliche", liberamente disponibili sul nostro sito web BT esterno.
		Internal/Confidential	Il contenuto dei messaggi è limitato al principio della necessità e le informazioni indicate di seguito non devono mai essere divulgate: · **Qualsivoglia informazioni sulle carte di pagamento.** · **Coordinate bancarie.** · **PIN o altre password.** · **Dati personali.**
		Highly Confidential	Non consentito.

3.2 Gestione dei documenti cartacei.

Riferimento	Cosa si desidera fare con queste informazioni?	Classificazione	Requisiti di gestione
HPD10	Voglio salvare, copiare, stampare o lavorare su informazioni in formato cartaceo in ufficio.	Internal/Confidential	Le Informazioni BT non dovrebbero essere utilizzate in formato cartaceo se non specificato nell'ambito del lavoro o approvato dallo Stakeholder BT. A seguire, si applicano queste indicazioni: Prendere tutte le misure di protezione necessarie a prevenire divulgazioni accidentali. Quando non vengono utilizzate, e quando gli uffici sono chiusi, le informazioni devono essere riposte e conservate in un'area a cui possa accedere esclusivamente il personale autorizzato, come degli armadietti, cassetti chiusi a chiave o locali ad accesso limitato. Utilizzare una stampante con controllo degli accessi, una stampante collegata a un PC o una stampante in un locale ad accesso controllato e verificare di aver inviato i dati alla stampante corretta. Usare la funzione di stampa protetta per recuperare il materiale stampato dalla stampante, a meno non se ne possa garantire un prelievo immediato.
		Highly Confidential	Non consentito
HPD20	Voglio stampare mentre mi trovo in un Edificio BT	Internal/Confidential	Verificare che la stampante a cui si inviano i documenti sia corretta e non lasciare i documenti nel vassoio di stampa. Utilizzare una stampante con controllo degli accessi, una stampante collegata a un PC o una stampante in un locale ad accesso controllato.
		Highly Confidential	Come le informazioni "Internal/Confidential"

HPD30	Voglio copiare o stampare delle informazioni che non si trovano presso la sede della terza parte o nella mia abitazione (ad esempio, si trovano presso la sede del subappaltatore, in un hotel, ecc.)	Internal/Confidential	Non consentito.
		Highly Confidential	Non consentito.
HPD40	Voglio portare una copia cartacea delle informazioni fuori da un ufficio BT, dalla Sede di una terza parte o un Negozio	Internal/Confidential	**Non è consentito rimuovere i dati di pagamento e/o dei clienti BT dagli uffici di BT, le Sedi delle terze parti o i negozi.** Esistono altre tipologie di informazioni che non devono mai essere rimosse, se non specificato nell'ambito del lavoro o approvato dallo Stakeholder BT. A seguire, si applicano queste indicazioni: Operare nel rispetto della *due diligence*. Prendere tutte le misure di protezione necessarie a prevenire una compromissione accidentale (ad esempio, trasportare il materiale in una borsa o carpetta opaca). Mai lasciare il materiale incustodito. In caso di smarrimento, è necessario aprire una pratica di incidente di sicurezza e comunicarlo al proprio Stakeholder BT nel più breve tempo possibile.
		Highly Confidential	Non consentito

HPD50	Voglio condividere o inviare una copia cartacea delle informazioni a parti interne.	Internal/Confidential	Le Informazioni BT non dovrebbero essere utilizzate in formato cartaceo se non specificato nell'ambito del lavoro o approvato dallo Stakeholder BT. A seguire, si applicano queste indicazioni: Riporre il documento all'interno di una busta a uso interno o di una busta senza finestra da consegnare a mano o per posta, servendosi del sistema di posta interno. Non inviare il materiale alle abitazioni delle parti interne. Non indicare il livello di classificazione all'esterno della busta. Se le informazioni sono coperte da "segreto professionale", attenersi alle linee guida del proprio ufficio legale In caso di smarrimento, è necessario aprire una pratica di incidente di sicurezza e avvisare il proprio Stakeholder BT nel più breve tempo possibile.
		Highly Confidential	Non consentito
HPD60	Voglio condividere o inviare una copia cartacea delle informazioni a parti esterne	Internal/Confidential	Non consentito
		Highly Confidential	Non consentito
HPD70	Voglio spedire un fax	Internal/Confidential	Inviare una copertina con una pagina di prova e contattare il destinatario per verificare l'avvenuta ricezione prima di inviare i documenti a mezzo fax. Se le informazioni sono coperte da "segreto professionale", attenersi alle linee guida del proprio ufficio legale.
		Highly Confidential	Non consentito

HPD80	Voglio eliminare le informazioni su formato cartaceo	Internal/Confidential	Accertarsi che le informazioni non debbano essere conservate per motivi legali o normativi. Nel rispetto di quanto indicato nella norma DIN66399 / livello P4, distruggere i documenti in particelle di dimensioni minime servendosi di una distruggidocumenti (sono comprese le informazioni sulle carte di pagamento). Mai gettare questi documenti in un cestino della spazzatura generale.
		Highly Confidential	Nessuno dovrebbe essere in possesso di una copia cartacea di questa classificazione delle informazioni. Qualora esistessero copie cartacee, attenersi alle indicazioni seguenti: Accertarsi che le informazioni non debbano essere conservate per motivi legali o normativi. Nel rispetto di quanto indicato nella norma DIN66399 / livello P4, distruggere i documenti in particelle di dimensioni minime servendosi di una distruggidocumenti (sono comprese le informazioni sulle carte di pagamento) oppure, conformemente alla norma BS EN15713:2009, si potrebbe procedere all'incenerimento. Mai gettare questi documenti in un cestino della spazzatura generale. **NB: Alcune informazioni potrebbero richiedere la distruzione del materiale in loco da parte di una terza parte esterna certificata. In tal caso, tale terza parte è tenuta a consegnare un certificato che attesti l'avvenuta distruzione.**

3.3 Gestione dei documenti elettronici.

Riferimento	Cosa si desidera fare con queste informazioni?	Classificazione	Requisiti di gestione
HED10	Voglio archiviare informazioni elettroniche sul mio PC/laptop aziendale	Tutti i dati BT	Le copie di lavoro possono essere conservate sul proprio laptop aziendale solo se è prevista la crittografia integrale del disco, ad esempio tramite un prodotto come Bitlocker. Questo strumento converte le informazioni in codici illeggibili che non possono essere decifrati facilmente da persone non autorizzate. I documenti completati devono essere archiviati in sicurezza e le copie di lavoro devono essere rimosse dal laptop.
HED20	Desidero salvare i miei documenti su un sistema di gestione documentale, come SharePoint o su un'unità di rete	Internal/Confidential	Limitare la possibilità di modificare il sito e i documenti ai soli soggetti autorizzati. L'amministratore o proprietario del sistema di gestione documentale / unità di rete deve: - Utilizzare i gruppi e i livelli di autorizzazione per impostare un controllo degli accessi basato su ruoli. Questi devono essere impostati non oltre il livello minimo necessario alle persone per eseguire il proprio lavoro. - Revisionare i controlli degli accessi ogni anno. - Documentare il processo in modo da assegnare i soggetti ai ruoli. - Le assegnazioni dei ruoli devono essere revisionate a intervalli regolari, preferibilmente su base trimestrale. **NOTA: i sistemi di gestione documentale o le unità di rete non devono essere utilizzati per l'archiviazione delle informazioni sulle carte di pagamento**

		Highly Confidential	Come le informazioni "Internal/Confidential" e: Crittografare i documenti prima di caricarli nel sistema di gestione documentale. Si dovrebbe anche impostare una data in cui l'accesso al documento sarà revocato. **NOTA: i sistemi di gestione documentale o le unità di rete non devono essere utilizzati per l'archiviazione delle informazioni sulle carte di pagamento**
HED30	Voglio archiviare informazioni elettroniche nel cloud o con servizi Internet (in assenza di un contratto commerciale di hosting delle Informazioni BT) come Google docs, GitHub, Drobox, Pastebin, Facebook, ecc.	Tutti i dati BT	Non consentito.
HED40	Voglio archiviare informazioni elettroniche su supporti amovibili come una chiavetta.	Tutti i dati BT	Consentito solo a chi ha un'esigenza commerciale autorizzata a fare uscire le Informazioni BT dall'ufficio, ma tutti i dispositivi e le informazioni devono essere crittografati. In caso di smarrimento, è necessario aprire una pratica di incidente di sicurezza e comunicarlo allo Stakeholder BT nel più breve tempo possibile. **NOTA: i supporti amovibili non devono essere utilizzati per l'archiviazione delle informazioni sulle carte di pagamento**
HED50	Voglio archiviare informazioni o documenti elettronici sul mio laptop o dispositivo personale.	Tutti i dati BT	Non consentito.
HED60	Voglio inviare documenti elettronici al mio indirizzo e-mail personale	Tutti i dati BT	Non consentito.
HED70	Voglio auto-inoltrare a un indirizzo e-mail esterno	Tutti i dati BT	Non consentito.

HED80	Voglio condividere o inviare dei documenti elettronici a parti interne	Internal/Confidential	Le Informazioni Internal/Confidential di BT devono essere condivise esclusivamente con parti interne, sulla base del principio della necessità, quando tali informazioni sono necessarie allo svolgimento del loro lavoro. È inoltre necessario: · Specificare che l'e-mail contiene Informazioni Internal/Confidential di BT. · Utilizzare le impostazioni di sensibilità per contrassegnare l'e-mail come "Confidential" · Impostare le autorizzazioni su "Non inoltrare" **NOTA: Le informazioni sulle carte di pagamento non dovrebbero mai essere conservate su un PC ma in caso sia necessario farlo (compreso l'invio tramite e-mail) devono essere sempre crittografate.**
		Highly Confidential	Le Informazioni Highly Confidential di BT devono essere condivise esclusivamente con parti interne, sulla base del principio della necessità, quando tali informazioni sono necessarie allo svolgimento del loro lavoro. È inoltre necessario: · Specificare che l'e-mail contiene Informazioni Highly Confidential di BT. · Utilizzare le impostazioni di sensibilità per contrassegnare l'e-mail come "Highly Confidential" · L'ideale sarebbe impostare le autorizzazioni su "Non inoltrare" · Usare la posta elettronica sicura per l'invio (se la funzione non è disponibile, crittografare le informazioni) **NOTA: Le informazioni sulle carte di pagamento non dovrebbero mai essere conservate su un PC ma in caso sia necessario farlo (compreso l'invio tramite e-mail) devono essere sempre crittografate.**

HED90	Voglio condividere o inviare dei documenti elettronici a parti esterne	Tutti i dati BT	I documenti possono essere condivisi con o inviati a una parte esterna solo se sussiste un'esigenza commerciale approvata o in presenza di un altro giustificativo, come un NDA. · I documenti possono essere condivisi con o inviati a una parte esterna solo nel rispetto del principio della necessità, qualora sussista un'esigenza commerciale, contrattuale o legislativa approvata e previa autorizzazione dello Stakeholder BT. - Accertarsi che in tutti i documenti e in tutte le e-mail sia indicato il livello di classificazione dei dati. · Accertarsi che la parte esterna conosca il livello di classificazione dei documenti e i requisiti di protezione. · Crittografare le informazioni · Verificare che l'indirizzo e-mail di destinazione sia corretto. - Ove applicabile, è comunque richiesto il rispetto delle linee guida dell'ufficio legale sul segreto professionale.
HED91	Voglio inviare un'e-mail a un gruppo ampio di dipendenti BT (più di 100), (ad esempio per fare un sondaggio tra i dipendenti, inviare materiale formativo, informazioni sui benefit)	Internal/Confidential	Attenersi alla nostra Guida per terze parti relativa ai briefing tramite e-mail
		Highly Confidential	Non consentito
HED100	Voglio trasferire internamente un documento BT o informazioni BT senza utilizzare l'e-mail, Skype/Lync for Business o supporti amovibili (ad esempio perché il file è troppo pesante)	Tutti i dati BT	È possibile utilizzare una soluzione di trasferimento file tramite Internet approvata dalla propria Politica di sicurezza. Crittografare il documento alla fonte prima di caricarlo.

HED110	Voglio trasferire esternamente un documento BT o informazioni BT senza utilizzare l'e-mail, Skype/Lync for Business o supporti amovibili (ad esempio perché il file è troppo pesante)	Internal/Confidential	I documenti possono essere condivisi con o inviati a una parte esterna solo se sussiste un'esigenza commerciale approvata o in presenza di un altro giustificativo, come un NDA, previa approvazione dello Stakeholder BT · I documenti possono essere condivisi con o inviati a una parte esterna solo nel rispetto del principio della necessità, qualora sussista un'esigenza commerciale, contrattuale o legislativa approvata e previa autorizzazione del proprietario o del creatore del documento. · I dati devono essere protetti quando si trovano nell'ambiente esterno per evitare che se ne perda la riservatezza, l'integrità o la disponibilità · Le informazioni devono essere crittografate prima dell'invio o in fase di trasmissione tra il proprio ambiente e quello esterno. - Accertarsi che in tutti i documenti sia indicato il livello di classificazione dei dati. · Accertarsi che il destinatario sia corretto. · Utilizzare un protocollo di trasferimento in rete standard come l'FTP.

		Highly Confidential	I documenti possono essere condivisi con o inviati a una parte esterna solo se sussiste un'esigenza commerciale approvata o in presenza di un altro giustificativo, come un NDA. · I documenti possono essere condivisi con o inviati a una parte esterna solo nel rispetto del principio della necessità, qualora sussista un'esigenza commerciale, contrattuale o legislativa approvata e previa autorizzazione dello Stakeholder BT. · Utilizzare la crittografia end-to-end completa per proteggere i dati dalla fonte (proprio sistema) alla destinazione (sistema esterno) e quando sono inattivi una volta giunti nel sistema della terza parte conformemente ai requisiti indicati nello Standard di terzi - Sezione 11. - Accertarsi che in tutti i documenti sia indicato il livello di classificazione dei dati. · Accertarsi che il destinatario sia corretto. · Utilizzare un protocollo di trasferimento in rete standard come l'FTP.
HED120	Voglio eseguire il backup dei miei documenti elettronici	Tutti i dati BT	· I documenti BT andrebbero archiviati solo sulle unità di rete o sui sistemi di gestione documentale approvati dal proprio team INFOSEC. (Se l'unica opzione consiste nell'usare supporti amovibili, il dispositivo deve essere crittografato) · Tutti i contenuti devono essere crittografati o protetti da password.
HED130	Voglio eliminare i documenti elettronici	Tutti i dati BT	I documenti conservati su SharePoint e nelle unità di rete devono essere eliminati utilizzando le funzioni di eliminazione standard di Windows.

			Le pattumiere per la raccolta differenziata devono essere svuotate almeno una volta alla settimana. (Ciò non si applica agli ambienti Citrix, ad esempio i back office del settore retail e i call centre offshore, poiché sono gestiti in automatico) Le e-mail non più necessarie devono essere eliminate.
HED140	Voglio smaltire o riutilizzare delle apparecchiature IT che hanno contenuto Informazioni BT Confidential/Highly Confidential, ad esempio componenti, attrezzature di terzi, backup, componenti server mandati indietro in riparazione	Tutti i dati BT	I servizi di distruzione possono essere utilizzati per molti tipi di supporti e hardware, come gli HDD, il nastro magnetico, le microfiche, CD/DVD, i circuiti stampati e i dispositivi di telefonia mobile Conservare un registro delle apparecchiature distrutte. I servizi di cancellazione dati possono essere utilizzati per le apparecchiature destinate al riutilizzo. Conservare un registro delle apparecchiature da cui i dati sono stati cancellati e richiedere un certificato che attesti l'avvenuta cancellazione dei dati. Se nelle apparecchiature erano contenuti dati del governo britannico, **DEVE** essere usato Blanco, ovvero l'unico prodotto certificato.
HED150	Voglio eliminare i dati di sistema e delle applicazioni	Tutti i dati BT	I dati devono essere eliminati a un livello sufficiente affinché non siano più recuperabili. È preferibile utilizzare un metodo basato su software di eliminazione dati (eventualmente definito di cancellazione, rimozione o distruzione dati) per sovrascrivere i dati.

			I backup da conservare per legge devono essere consultabili in qualsiasi momento.

3.4 Gestione dei dati di sistema e delle applicazioni (dati elettronici).

Per dati elettronici si intendono tutti i dati e le informazioni conservati nei sistemi o nelle applicazioni gestite dal reparto tecnologia o dalle singole business unit, come i data warehouse o i sistemi di fatturazione.
I dati estratti da un'applicazione o un sistema ricevuti da una persona devono essere trattati come un documento elettronico (cfr. Sezione 6.3).

Riferimento	Cosa si desidera fare con questi dati e informazioni?	Classificazione	Requisiti di gestione
HSADE	Voglio salvare e trattare informazioni e dati elettronici di BT in un data centre (incluso il Cloud e una Terza parte)	Tutte le Informazioni BT	Attenersi alle procedure di controllo indicate nello Standard di Terzi Se i dati comprendono informazioni sulle carte di pagamento, devono essere conservati nel rispetto dei requisiti indicati nello standard PCI DSS. Se i dati comprendono informazioni sulle coordinate bancarie, essendo particolarmente sensibili, sarà necessario implementare i seguenti controlli. 1. I conti bancari delle persone fisiche devono essere sottoposti a tokenizzazione (conti bancari personali di clienti e dipendenti). 2. Se vengono mostrati i dettagli di un conto bancario a un agente nell'ambito di una procedura commerciale (ad esempio, per verificare la correttezza di un conto per la fatturazione, quando si comunica con un cliente tramite e-mail oppure su una fattura), devono essere mostrate solo le ultime 4 cifre (ovvero dettagli del conto bancario mascherato). 3. Qualora fosse necessario accedere all'intero conto bancario (ad

			esempio, per abilitare una richiesta di debito o di credito da una banca), i dati devono essere de-tokenizzati o decrittografati, poi trasferiti alla banca usando un meccanismo di trasporto crittografato. Non appena le coordinate bancarie de-tokenizzate e decrittografate saranno state usate, dovranno essere eliminate in tutta sicurezza.
HSAD1	Voglio salvare e trattare informazioni e dati elettronici BT in un'applicazione o un sistema di terzi	Tutti i dati	· Tutte le Informazioni Confidential/Highly Confidential e i dati personali devono essere crittografati. · Le informazioni sulle carte di pagamento devono essere crittografate conformemente a quanto indicato nello standard PCI DSS.
HSAD2	Voglio inviare informazioni e dati elettronici usando una rete di terzi o all'esterno	Tutti i dati BT	Prima di poter rilasciare dei materiali è necessario ottenere l'approvazione di uno Stakeholder BT La terza parte deve aver sottoscritto un NDA o un adeguato contratto. I dati trasferiti devono essere crittografati. In caso di trasferimento di Informazioni Confidential/Highly Confidential, inclusi i dati personali, a una terza parte al di fuori della propria rete, è richiesta la sottoscrizione di un 'Accordo sul trattamento dei dati' (Data Processing Agreement) .

4. Conservazione delle Informazioni.

Le Terze parti dovrebbero avere una 'Politica sulla conservazione dei dati' che disciplini questa attività, contenente un "Programma di conservazione delle informazioni" specifico in cui devono essere definiti i periodi di conservazione delle Informazioni BT. (Le Informazioni dovrebbero essere conservate per il tempo necessario a eseguire il Contratto, dopo il quale non dovrebbero essere conservate per più di un massimo di due anni, a meno che non sia stato concordato un periodo di conservazione diverso tra BT e la terza parte, o non sia richiesto da eventuali leggi applicabili.)

Informazioni BT - in qualsiasi forma, documenti digitali o cartacei classificati come record o non-record, come tutte le copie di lavoro, le bozze, appunti informali, e-mail spam o altre forme di archiviazione (come microfiche / microfilm, pellicola fotografica, registrazioni audio o video).

5. Smaltimento delle Apparecchiature.

Tutte le apparecchiature su cui è possibile salvare i dati, compresi i componenti di computer, devono essere trattati come Asset informativi. Esempi di 'Asset informativi' sono disponibili nel Glossario che segue.
Tutte le apparecchiature devono essere smaltite al termine della loro vita operativa. Seguono esempi di termine della vita operativa:

- Il prodotto è guasto
- Il prodotto è stato dismesso (ritirato dal servizio o non più necessario)
- Il prodotto è stato utilizzato in un collaudo o un Proof of Concept

5.1 Requisiti relativi allo Smaltimento per Terze parti.

Questa sezione si applica a:

- Qualsivoglia terza parte o agenzia subappaltata.
- Qualsivoglia terza parte che presta servizi di manutenzione per le apparecchiature di BT da cui gli Asset informativi potrebbero essere rimossi e sostituiti nell'ambito del servizio.
- Qualsivoglia terza parte che fornisce servizi in outsourcing a BT, nell'ambito dei quali i dati BT si trovano negli archivi o nelle apparecchiature delle terze parti.
- Qualsivoglia servizio di smaltimento rifiuti incaricato di smaltire le apparecchiature di BT.

Riferimento	Cosa si desidera fare con questi dati e informazioni?	Classificazione	Requisiti di gestione
EDR10	Voglio smaltire le apparecchiature che contengono i Dati BT.	Tutti i dati BT	Dischi rigidi (HDD) - Cancellazione, disintegrazione o incenerimento con metodo "Multi Pass"
			Unità allo stato solido (SSD) - Cancellazione, disintegrazione con metodo "Multi Pass"
			CD-R / DVD-R, CD-RW / DVD-RW, BD-R, BD-RE, BD-RE - Abrasione, disintegrazione, incenerimento

			Nastro magnetico - Smagnetizzazione, disintegrazione, incenerimento
			Unità Flash e USB - Cancellazione, smagnetizzazione, disintegrazione con metodo “Multi Pass”
			SIM - Tagliarle in tanti piccoli pezzi (attraverso il contatto metallico) per renderle illeggibili.

6. Requisiti di Audit.

6.1 Requisiti di audit per l’eliminazione di dati e informazioni

È necessario mantenere registri completi relativi alla conservazione e all’eliminazione dei dati, corredati di *audit trail*, prove e sistemi di monitoraggio. Tali registri devono comprendere:

- Prova dell’avvenuta distruzione e/o eliminazione (inclusa la data di presa in carico e il metodo utilizzato)
- Audit log dei sistemi per l’eliminazione.
- Certificati di avvenuta eliminazione dei dati.
- Chi si è occupato dell’eliminazione (compresi eventuali collaboratori / terzi o appaltatori addetti all’eliminazione)?
- La generazione di un report di distruzione e verifica a conferma dell’esito positivo o negativo della procedura di eliminazione / distruzione. (dal processo di sovrascrittura deve essere generato un report in cui vengono specificati i settori che non è stato possibile cancellare).

6.2 Requisiti di audit per lo smaltimento delle apparecchiature

Per i seguenti tipi di apparecchiature deve essere fornito un *audit trail*:

- Supporti amovibili.
- Unità disco.
- Nastri per backup.
- Componenti per computer (cfr. Glossario).

È necessario conservare registri completi atti a fornire un *audit trail* che includa come minimo:

- Il nome dell’applicazione o del servizio che ha utilizzato quell’apparecchiatura.
- Il tipo di apparecchiatura, come un computer desktop, laptop, un server, un nastro, un router, ecc.
- Il numero di dischi rigidi contenuti nell’apparecchiatura (se applicabile).
- L’apparecchiatura identificata dal numero di serie.
- I componenti dell’apparecchiatura identificati dal numero di serie.
- Un tracciamento delle risorse completo relativo a tutte le apparecchiature e ai componenti per l’intero ciclo di vita dell’apparecchiatura smaltita.

- Prova dell'avvenuta distruzione e/o eliminazione (inclusa la data di presa in carico e il metodo utilizzato)
- Dati relativi al soggetto che si è occupato dello smaltimento (compresi eventuali collaboratori addetti allo smaltimento / terzi / appaltatori addetti allo smaltimento rifiuti)?
- Report di avvenuta distruzione e verifica generati per confermare l'esito positivo o negativo della procedura di distruzione o raccolta/differenziazione rifiuti. Ad esempio, dal processo di sovrascrittura deve essere generato un report in cui vengono specificati i settori che non è stato possibile cancellare. Questi report dovrebbero includere la capacità, la marca, il modello e il numero di serie dei supporti.

7. Glossario.

Termine	Spiegazione
Terzo/Terza parte	Tutte le società coinvolte nel trattamento di dati/informazioni BT e nella gestione delle apparecchiature di BT devono operare nel rispetto di questo standard. Questa voce include: · Qualsivoglia terzo o agenzia subappaltata · Qualsivoglia terzo che presta servizi di manutenzione per le apparecchiature di BT da cui gli Asset informativi potrebbero essere rimossi e sostituiti nell'ambito del servizio · Qualsivoglia terzo che fornisce servizi in outsourcing a BT, nell'ambito dei quali i dati BT si trovano negli archivi o nelle apparecchiature di terzi · Qualsivoglia servizio di smaltimento rifiuti incaricato di smaltire le apparecchiature di BT
AES	Advanced Encryption Standard
Chiavi asimmetriche	La crittografia asimmetrica, detta anche crittografia a chiave pubblica, si serve di chiavi pubbliche e private per crittografare e decrittografare i dati. Le chiavi non sono altro che dei grandi numeri abbinati tra loro ma non identici (asimmetrici). Una delle chiavi della coppia può essere condivisa con chiunque e prende il nome di chiave pubblica.
Dati BT	Tutti i dati che sono di proprietà di o concessi in licenza da BT per operare in qualità di *Limited Company* nel Regno Unito o una delle sue controllate nel mondo.
CDP	Punto di distribuzione elenco revoche di certificati (Certificate Revocation List Distribution Point)
CESG	Communications-Electronics Security Group del governo britannico.
Componenti per computer	Controller per dischi rigidi, per unità CD-ROM, DVD, schede di interfaccia Ethernet, controller per schermi di computer e stampanti in rete.
CRL	Certificate Revocation List
Cliente	Una persona fisica o giuridica che ottiene, ha ottenuto, o che secondo BT o uno dei suoi brand è probabile che ottenga prodotti o riceva offerte per prodotti o servizi.
Dati dei clienti	Qualsivoglia dato relativo ai clienti dei brand gestiti da BT.

Dati	Parole, numeri, dati, immagini, suoni, ecc. senza contesto.
Eliminazione dei dati	L'eliminazione dei dati consiste nella distruzione di tutti i dati e di tutte le informazioni non classificati come record permanente.
Ciclo di vita dei dati	Il ciclo di vita dei dati copre la loro raccolta, il salvataggio, la gestione, il trattamento, la trasmissione e la distruzione.
Periodo di conservazione dei dati	Si tratta del periodo (che potrebbe essere permanente) durante il quale una tipologia di dato o informazione rimane conservata/salvata prima di poter essere distrutta o eliminata. Durante questo periodo in cui i dati possono essere archiviati e sono accessibili fino alla fine del periodo stesso.
DEK	Data Encryption Key (Chiave di crittografia dati)
Dati elettronici	Per dati elettronici si intendono tutti i dati e le informazioni conservati nei sistemi o nelle applicazioni gestite dal reparto tecnologia o dalle singole business unit, come i data warehouse o i sistemi di fatturazione.
Chiave a curva ellittica	Crittografia a curva ellittica. La crittografia a curva ellittica (ECC) è un approccio di crittografia a chiave pubblica basato sulla struttura algebrica delle curve ellittiche su campi finiti. L'ECC richiede chiavi più piccole rispetto alla crittografia non EC (basata su campi di Galois semplici) per offrire livelli di sicurezza equivalenti
Crittografia	Conversione dei dati in un codice segreto affinché non possano essere letti da un soggetto non autorizzato.
Entropia	Misurazione della casualità dei dati; una chiave a 128 bit può avere un massimo di 128 bit di entropia, o come minimo 1.
GCM	Google Cloud Messaging
HSM	Hardware security-module (Modulo di sicurezza hardware)
Record inattivo	I record possono essere in stato attivo o inattivo. Quando un record attivo scade o non è più richiesto, ad esempio quando un cliente lascia BT, il relativo record cliente diventa inattivo mentre se un dipendente lascia BT il relativo record HR diventa inattivo.
Informazioni	Una raccolta di parole, numeri, date, immagini, suoni, ecc. inseriti in un contesto che dà loro un significato.
Asset informativo	Tutte le apparecchiature su cui è possibile salvare i dati sono definite Asset informativi. Alcuni esempi sono: Unità disco (allo stato solido e magnetiche), supporti amovibili (ad esempio, floppy disk, USB, DVD, CD, schede di memoria interne, flash card e schede SD), nastri per il backup, schede SIM per telefoni mobili. I componenti per computer come i controller per dischi rigidi, per unità CD-ROM, DVD, le schede di interfaccia Ethernet, i controller per schermi di computer e le stampanti in rete.
Sistemi informativi	Una raccolta di hardware, software, dati, persone e procedure che collaborano per produrre informazioni di qualità.
KEK	Key Encryption Key (Chiave di crittografia chiave)
NDA	Non-Disclosure Agreement (Accordo di riservatezza)
NIST	National Institute of Standards and Technology

Nonce	Un numero casuale generato e utilizzato solo una volta durante uno scambio di crittografia, spesso per l'autenticazione.
Non-record	Duplicati di originali e di copie di lavoro. Documentazione interna relativa a questioni non commerciali. Bozze di lettere, report, fogli di lavoro e appunti informali. Libri, manuali e altri materiali stampati ottenuti da fonti esterne a BT come materiale di riferimento. Spam e posta indesiderata.
OCSP	Online Certificate Status Protocol
Ufficio	Fa riferimento a qualsivoglia sede BT, come un negozio di vendita al dettaglio, un call centre, una sede principale, un ufficio a uso generale.
Informazioni sulle carte di pagamento	Informazioni relative a un conto utilizzato dal titolare di una carta per effettuare pagamenti a un esercente. Esempi: numero di conto primario (PAN), data di scadenza, CVV. Il trattamento di queste informazioni è disciplinato dal regolamento PCI/DSS.
Dati personali	Informazioni relative a qualsivoglia persona fisica - compresi i clienti e chiunque lavori per BT - che includono, a titolo esemplificativo ma non esaustivo, il nome completo, la data di nascita, l'indirizzo e il numero di telefono.
PRNG	Pseudo-random number generator (Generatore di numeri pseudo-casuali)
Record/registro	Documenti conservati come prova delle transazioni commerciali di BT, delle sue decisioni, attività, e-mail o nel rispetto di obblighi legali. Sono altresì compresi i dati e le informazioni conservati nei sistemi o nelle applicazioni in quanto anch'essi contengono prove delle transazioni commerciali di EE, dei suoi prodotti e servizi.
RSA	Tecnologia di crittografia a chiave pubblica sviluppata da RSA Data Security, Inc. È l'acronimo di "Rivest, Shamir e Adelman"
Salted Hash (Hash sottoposti a salting)	In crittografia, un sale è un insieme di dati random usati come input aggiuntivo a una funzione unidirezionale che effettua l'hashing di una password o passphrase. Per maggiori informazioni, fare riferimento all'Appendice C.
Chiavi simmetriche	Gli algoritmi a chiave simmetrica vengono utilizzati per la crittografia che usa le stesse chiavi sia per crittografare il testo normale che per decrittografare il testo crittografato.
Politica di conservazione a livello di sistema	In una politica a livello di sistema viene specificato il periodo di conservazione dei dati nel rispetto dei Programmi di conservazione dati aziendali
TPM	Trusted Platform Module

8. Cronologia delle modifiche.

N. versione	Data	Modifica apportata da	Breve descrizione della modifica
4.0 bozza	05/08/2018	Karen Tanner	Bozza per sostituire la versione corrente 3
4.0 rilasciata	07/11/2019	Karen Tanner	Revisionata e approvata

N. versione	Data	Modifica apportata da	Breve descrizione della modifica

9. Approvazione documento.

Nome	Ruolo	Data
Ian Morton	Proprietario documento versione BT	07/11/2019

10. Conformità.

Siamo lieti che la maggior parte delle terze parti si comportino in modo professionale e in linea con i valori di BT. Tuttavia facciamo presente che, qualora dovessimo riscontrare un comportamento non adeguato al presente standard o a qualsivoglia altra politica o standard, potremmo decidere di risolvere gli accordi presi relativamente alla prestazione dei servizi.

11. Proprietà e Riservatezza.

Il presente documento non deve essere condiviso con nessun'altra terza parte senza l'autorizzazione scritta di BT. Il presente standard e tutti i documenti associati sono di proprietà di BT e, se richiesto, devono essere restituiti.