

ALFA SRL	PIANO DELL'AUDIT	Rev.0 del 16-01-2024 Pag. 1 di 1
-----------------	-------------------------	--

Organizzazione: ALFA SRL		Data audit: 18-10-24	Ora di inizio: 9.00	Sede: sede operativa Alfa srl
Auditor	Nome e Cognome: Dott.ssa Teresa Battaglia		Ruolo: DPO	
Obiettivo dell’audit	Audit iniziale di valutazione della conformità al GDPR			
Campo di applicazione	Promozione e vendita di contratti di utenza per conto delle principali imprese di telecomunicazioni nazionali ed internazionali			
Orario	Ambito		Funzioni coinvolte	
9.00	Riunione di apertura		Direzione –Amministratore di sistema- Consulente	
	Organigramma, nomine, ambiti di trattamento, istruzioni operative, formazione soggetti autorizzati al trattamento. Analisi dei rischi - DPIA e misure organizzative di mitigazione dei rischi		Direzione o un suo rappresentante	
	Informative agli interessati		Direzione o un suo rappresentante - Amministratore di sistema	
	Procedure data Breach		Direzione - Amministratore di sistema	
	Policies aziendali		Direzione - Amministratore di sistema	
	Misure tecniche di mitigazione dei rischi		Amministratore di sistema	
13.00	Riunione di chiusura		Direzione – DPO -Amministratore di sistema- Consulente	

DATA 12/10/2024

FIRMA: *Teresa Battaglia*

Processo/Funzione auditati: DIREZIONE

ELEMENTO DI CONTROLLO	Rif. Normativo	EVIDENZA OGGETTIVA	ESITO
Ruoli e responsabilità	Artt. 4, 24, 28 e considerando 74-78 GDPR	Organigramma aggiornato al 15/07/2024 comprensivo di tutte le figure individuate dal GDPR. Tra i soggetti autorizzati al trattamento <i>Sig. Mario Rossi</i>	C
Nomine formali soggetti autorizzati al trattamento	Art 4 GDPR	Nomina a soggetto autorizzato al trattamento <i>Sig.ra Maria Bianchi</i> del 17/01/2024 – ambito di trattamento addetto ufficio commerciale – istruzioni operative in Rev.0 del 16-01-2024 firmate per ricevuta all'atto della nomina il 17/01/2024.	C
Nomine formali Responsabili del trattamento esterno (Sub-Responsabili)	Art. 28 GDPR	Nomina società di medicina del lavoro <i>Prevention Srl</i> del 15/04/2024	
L'amministratore di sistema	Allegato B Codice Privacy, Prov. 27 novembre 2008	Nomina Ing. Ciro Esposito del 20/02/2024 – Registro Amministratore di sistema ultima registrazione del 02-10-2024	C
Formazione	Art. 29 GDPR	Piano Annuale di formazione 2024 del 22/01/2024 Verbale di formazione del 25/01/2024 sul GDPR rivolto a tutto il personale della durata di 4 ore	C
Registro dei trattamenti	Art. 30 GDPR	Registro dei trattamenti in Rev.0 del 16-01-2024	C
Analisi dei Rischi	Artt. 24, 25, 32	Analisi dei Rischi in Rev.0 del 16-01-2024	C
DPIA	Art. 35 GDPR, linee guida WP29	DPIA in Rev.0 del 16-01-2024 per videosorveglianza	C
Misure organizzative	Artt. 25, 32 GDPR	Controllo accessi: registro Visitatori ultima registrazione del 17/10/2024 Avv. Anna Di Legge ingresso ore 11.30 uscita ore 12.45	C
		Trattamento cartaceo Istruzione operativa in Rev.0 del 16-01-2024 consegnata ai soggetti autorizzati – Vista consegna <i>Sig.ra Maria Bianchi</i> del 17/01/2024	C
Informative agli interessati	Artt. 13, 14 GDPR	Informativa clienti in Rev.0 del 16-01-2024 Informativa dipendenti in Rev.0 del 16-01-2024 Informativa fornitori in Rev.0 del 16-01-2024 Informativa sito web in Rev.1 del 5-06-2024	C
Procedura di data Breach	Artt. 33, 34 GDPR	Procedura di data Breach in Rev.0 del 16-01-2024	C

ALFA SRL	LISTA DI RISCONTRO		Rev.0 del 16-01-2024 Pag. 2 di 2
	Art. 33 GDPR	Registro Data Breach senza registrazioni (non si sono verificati eventi)	C
LEGENDA: C = conforme NC = non conforme OSS = osservazione			
NOTE:			
Data: 18/10/2024		Firma Auditor: <i>Teresa Battaglia</i>	

Processo/Funzione auditati: Misure tecniche di mitigazione dei rischi /AMMINISTRATORE DI SISTEMA

ELEMENTO DI CONTROLLO	Rif. Normativo	EVIDENZA OGGETTIVA	ESITO
Politiche per la sicurezza delle informazioni	5.1 Annex A	Politica generale di sicurezza delle informazioni in Rev.0 del 16/01/2024 Elenco Policies aziendali del 16/01/2024 Analisi del contesto e delle parti interessate in rev.0 del 16/01/2024 SOA (Dichiarazione di applicabilità dei controlli) in rev.0 del 16/01/2024 Analisi dei rischi di sicurezza delle informazioni in rev.0 del 16/01/2024 Organigramma aggiornato al 15/07/2024 Mansionario in rev.0 del 16/01/2024	C
Ruoli e responsabilità della sicurezza delle informazioni	5.2	Organigramma aggiornato al 15/07/2024	C
Separazione dei compiti	5.3	Mansionario in rev.0 del 16/01/2024	C
Responsabilità di gestione	5.4	Nomina DPO del 18/01/2024 e comunicazione al garante del 22/01/2024 Nomina a soggetto autorizzato al trattamento Sig.ra Maria Bianchi del 17/01/2024 Nomina amministratore di sistema Ing. <i>Ciro Esposito</i> del 17/01/2024	C
Contatto con le autorità	5.5	Nomina DPO del 18/01/2024 e comunicazione al garante del 22/01/2024	C
Contatti con gruppi di interesse speciale	5.6	Contratto con il <i>dott. Luca Pacioli</i> del 24/11/2023 per la consulenza GDPR Contratto con l'azienda <i>Bill Gates Informatica Srl</i> del 12/12/2020 per assistenza tecnica e sistemistica Iscrizione alle newsletter di Federprivacy – Iusprivacy e Cybersecurity – ultima newsletter del 04/10/2024	C
Intelligence sulle minacce	5.7	Analisi dei rischi di sicurezza delle informazioni in rev.0 del 16/01/2024 Piano di formazione 2024 e Verbale di Formazione n.3 del 12/02/2024 sulle minacce alla sicurezza e contromisure da adottare	C
Sicurezza delle informazioni nella gestione dei progetti	5.8	Le attività vengono espletate su CRM fornito dalla società di telecomunicazioni committente (l'organizzazione è un'agenzia monomandataria). Requisiti di sicurezza stabiliti e garantiti dal committente.	C

Inventario di informazioni e altri beni associati	5.9	POL-3 Politica gestione asset in Rev. 0 del 12-01-24 Mod. 6.1.2.1 Classificazione degli Asset del 12-01-24	C
Uso accettabile delle informazioni e di altre risorse associate	5.10	POL-1 Politica Uso accettabile in Rev. 0 del 12-01-24 (es. par. 4.1 Uso del computer – 4.3 Utilizzo di Internet e della posta elettronica) Registro assegnazione degli asset ultimo aggiornamento consegna PC al sig. Giulio Ripamonti del 30-09-24	C
Restituzione di beni	5.11	Istruzione operativa I.O. 5.11 Riconsegna degli asset Registro riconsegna asset ultimo aggiornamento consegna PC sig.ra Eleonora Rossetti del 25-09-24	C
Classificazione delle informazioni	5.12	PROCEDURA PR 6.1.2 VdR sicurezza dati in Rev.0 del 12-01-2024 Mod. 6.1.2.1 Classificazione degli Asset del 12-01-24	C
Etichettatura delle informazioni	5.13	PROCEDURA PR 6.1.2 VdR sicurezza dati in Rev.0 del 12-01-2024 Mod. 6.1.2.1 Classificazione degli Asset del 12-01-24	C
Trasferimento di informazioni	5.14	Istruzione operativa allegata alla nomina per soggetto autorizzato al trattamento in Rev.1 del 15/07/2024	C
Controllo accessi	5.15	POL-2 POLITICA CONTROLLO ACCESSI in Rev.0 del 12-01-2024 Screen shot: di schermata di login PC Mac Mini assegnato al sig. Giulio Ripamonti	C
Gestione dell'identità	5.16	POL-2 POLITICA CONTROLLO ACCESSI in Rev.0 del 12-01-2024 Autenticazione a due fattori sig. Giulio Ripamonti su software gestionale CRM	C
Informazioni di autenticazione	5.17	POL-2 POLITICA CONTROLLO ACCESSI in Rev.0 del 12-01-2024 Screen shot di e-mail (protetta da pw) del 30-09-24 di assegnazione account al sig. Giulio Ripamonti con credenziali di accesso (user e pw).	C
Diritti di accesso	5.18	POL-2 POLITICA CONTROLLO ACCESSI in Rev.0 del 12-01-2024 Tentato accesso, dal PC della sig. ra Michela Rossi (segretaria) con livello di autorizzazione 1 (minimo), alla cartella "Contratti" condivisa dai livelli di autorizzazione 2 e 3. Accesso negato.	C
Sicurezza delle informazioni nei rapporti con i fornitori	5.19	Nomina a Sub Responsabile del fornitore del servizio Firewall del 20/12/2023 fornitore IG Informatica Srl	C
Affrontare la sicurezza delle informazioni negli accordi con i fornitori	5.20	Contratto fornitore IG Informatica Srl del 20/12/2023 completo di Clausole contrattuali di sicurezza dei dati trattati.	C

ALFA SRL	LISTA DI RISCONTRO		Rev.0 del 16-01-2024 Pag. 3 di 7
Gestire la sicurezza delle informazioni nella filiera ICT	5.21	POL-31 POLITICA DI SICUREZZA DEI FORNITORI in Rev.0 del 12-01-2024 Registro dei Fornitori qualificati 2024 Nomine a Sub Responsabili del trattamento per i trattamenti specifici.	C
Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori	5.22	Piano di Monitoraggio Fornitori 2024	C
Sicurezza delle informazioni per l'utilizzo dei servizi cloud	5.23	Documentazione di sicurezza del SAAS fornitore del gestionale CRM (Politica, informativa privacy compliance, certificazione ISO/IEC 27001 e ISO/IEC 27017)	C
Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni	5.24	POL-15 POLITICA DI GESTIONE DEGLI INCIDENTI DI SICUREZZA in Rev. 0 del 12/01/2024 PR. 10.2 GESTIONE NC ED AC	C
Valutazione e decisione sugli eventi di sicurezza delle informazioni	5.25	Registro Incidenti 2024 – nessun incidente registrato (non si sono verificati eventi che abbiano causato incidenti) Registro NC 2024 Registro AC 2024	
Risposta agli incidenti di sicurezza delle informazioni	5.26		
Imparare dagli incidenti di sicurezza delle informazioni	5.27		
Raccolta delle prove	5.28		
Sicurezza delle informazioni durante l'interruzione	5.29		
Prontezza ICT per la continuità aziendale	5.30	PR. 8.1.2 GESTIONE DELLA CONTINUITA' OPERATIVA Mod. 8.1.2.1 Piano di Continuità operativa 2024 Mod. 8.1.2.2 Programmazione test anno 2024 Mod. 8.1.2.3 verbale di esercitazione del 15-03-2024	OSS 1
Requisiti legali, statutari, regolamentari e contrattuali	5.31	Clausole contrattuali inserite nel contratto con il cliente Telefon del 12/01/2023 riguardanti la sicurezza delle informazioni	C
Diritti di proprietà intellettuale	5.32	N/A.	
Protezione dei registri	5.33	Le registrazioni sono protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato, come da contromisure a valle della valutazione dei rischi in Rev.0 del 16/01/2024	C
Privacy e tutela delle PII	5.34	<ul style="list-style-type: none">- Registro dei trattamenti Rev.0 del 16/01/2024- Nomina a soggetto autorizzato al trattamento Sig.ra Maria Bianchi del 17/01/2024- Nomina DPO del 18/01/2024 e comunicazione al garante del 22/01/2024 - Attestato di formazione corso sul GDPR per DPO e C.V. aggiornato al 18/01/24- Valutazione dei rischi in Rev.0 del 16/01/2024- Valutazione di impatto in Rev.0 del 16/01/2024- Informativa Dipendenti Sig.ra Michela Rossi con firma per rilascio consenso immagini videoregistrate-	C

ALFA SRL		LISTA DI RISCONTRO		Rev.0 del 16-01-2024 Pag. 4 di 7
Revisione indipendente della sicurezza delle informazioni	5.35	Programma annuale audit interni 2024 a cura del DPO	C	
Conformità a politiche, regole e standard per la sicurezza delle informazioni	5.36			
Procedure operative documentate	5.37	Elenco procedure del SGI in Rev.0 del 16/01/2024	C	
Controlli delle persone	6	Accordi contrattuali con i dipendenti relativamente alla sicurezza delle informazioni- accordi di riservatezza con i dipendenti – Visto contratto con la dipendente Michela Rossi del 15/12/2023 e nomina soggetto autorizzato	C	
Proiezione	6.1			
Termini e condizioni di lavoro	6.2			
Sensibilizzazione, istruzione e formazione alla sicurezza delle informazioni	6.3	Verbale di formazione del 25/01/2024 sul GDPR e sulla sicurezza delle informazioni rivolto a tutto il personale della durata di 4 ore Sistema disciplinare del 16-01-2024 per contravvenzione alle norme interne di sicurezza delle informazioni. Nessun richiamo al personale relativo alla sicurezza delle informazioni.		
Processo disciplinare	6.4			
Responsabilità dopo la cessazione o il cambio di rapporto di lavoro	6.5			
Accordi di riservatezza o non divulgazione	6.6			
Lavoro a distanza	6.7	N.A. (non viene effettuato smart working)		
Segnalazione di eventi di sicurezza delle informazioni	6.8	POL-30 POLITICA DI SEGNALAZIONE E GESTIONE DEGLI INCIDENTI Registro Incidenti 2024 – nessun incidente registrato (non si sono verificati eventi che abbiano causato incidenti)		
Controlli fisici	7	Il SGSI si applica a tutti i locali dell’organizzazione. E’ presente una porta blindata per l’accesso. I locali sono dotati di telecamere di sorveglianza e di allarme perimetrale esterno (i locali sono situati al piano terra con giardino) ed allarme antieffrazione su porta, finestre e balconi. Screen shot di ciò che viene inquadrato dalle telecamere di sicurezza. Screen shot del pannello di raccolta degli allarmi sulle minacce fisiche(intrusioni, movimenti, temperatura, umidità)	C	
Perimetri di sicurezza fisica	7.1			
Ingresso fisico	7.2			
Messa in sicurezza di uffici, locali e strutture	7.3			
Monitoraggio della sicurezza fisica	7.4			
Protezione contro le minacce fisiche e ambientali	7.5			
Lavorare in aree sicure	7.6			
scrivania e schermo protetti	7.7	Le scrivanie vengono ripulite in tempo reale dai documenti consultati. E’ presente il blocco schermo su tutti i PC (è richiesta la pw per accedere dopo l'interruzione) POL-13 POLITICA DI PROTEZIONE DELLA SCRIVANIA in Rev.0 del 12-01-24 POL-20 POLITICA DI SICUREZZA PER IL PC in Rev.0 del 12-01-24	C	

ALFA SRL	LISTA DI RISCONTRO	Rev.0 del 16-01-2024 Pag. 5 di 7
-----------------	---------------------------	-------------------------------------

Posizionamento e protezione delle apparecchiature	7.8	Non vengono utilizzati dispositivi portatili e mobili da remoto. La protezione da black out e picchi di corrente è rappresentata dai gruppi di continuità presenti presso ciascuna postazione.	C
Sicurezza dei beni fuori sede	7.9	POL-19 POLITICA DI GESTIONE DEI SUPPORTI DI MEMORIZZAZIONE in Rev.0 del 12-01-24	
Supporti di memorizzazione	7.10	Presente Contratto di assistenza per monitoraggio e manutenzione delle apparecchiature informatiche con azienda AT Informatica srl del 15/10/2023	
Utilità di supporto	7.11	Screen shot dell' applicazioni di controllo vita degli HD (software Easylife)	
Manutenzione delle apparecchiature	7.13	POL- 26 POLITICA PER IL TELEFONO CELLULARE	
Smaltimento o riutilizzo sicuro delle apparecchiature	7.14	POL-37 POLITICA DI BRING YOUR OWN DEVICE (BYOD) POL-21 POLITICA DI SMALTIMENTO DELLE APPARECCHIATURE	
Controlli tecnologici	8	Screenshot: di antivirus ABC e firewall a protezione dei PC	C
Dispositivi endpoint utente	8.1	POL-25 POLITICA PER SOFTWARE MALEVOLO E ANTIVIRUS in Rev.0 del 12-01-24	
Diritti di accesso privilegiati	8.2		
Limitazione dell'accesso alle informazioni	8.3		
Accesso al codice sorgente	8.4	N.A.	
Autenticazione sicura	8.5	POL-34 POLITICA DI GESTIONE DELLA CAPACITA' in Rev.0 del 12-01-24	C
Gestione della capacità	8.6	POL-35 POLITICA DI GESTIONE DELLA CONFIGURAZIONE in Rev.0 del 12-01-24	
Protezione contro i malware	8.7	POL-25 POLITICA PER SOFTWARE MALEVOLO E ANTIVIRUS in Rev.0 del 12-01-24	
Gestione delle vulnerabilità tecniche	8.8		
Gestione della configurazione	8.9	Screenshot: di antivirus ABC e firewall a protezione del server PR-6.1.2 Valutazione Rischio sicurezza in Rev.0 del 12-01-24 MOD. 6.1.2.3 PIANO DI TEST RETE E APPLICAZIONI 2024 MOD. 6.1.2.4 VULNERABILITY ASSESSMENT REPORT del 27-07-24 MOD. 6.1.2.5 PENETRATION TEST REPORT del 15-09-24	
Cancellazione delle informazioni	8.10	Per la formattazione a basso livello viene utilizzato il software XYZ Vista schermata software sul PC N.3	C
Mascheramento dei dati	8.11	POL-32 POLITICA DI DATA MASKING in Rev.0 del 12-01-24	
Prevenzione della fuga di dati	8.12		
Backup delle informazioni	8.13	Screenshot di Log di backup POL-7 POLITICA DI BACKUP E RIPRISTINO DEI DATI in Rev.0 del 12-01-24	C
Ridondanza delle strutture di elaborazione delle informazioni	8.14	I Log degli eventi vengono memorizzati e visualizzati mediante software dedicato.	C

ALFA SRL		LISTA DI RISCONTRO	Rev.0 del 16-01-2024 Pag. 6 di 7
Registrazione	8.15	Vista schermata dei Log registrati dal software KGQ negli ultimi 30 gg	
Attività di monitoraggio	8.16	POL-36 POLITICA DI GESTIONE DEI LOG FILE in Rev.0 del 12-01-24	
Sincronizzazione dell'orologio	8.17	La sincronizzazione avviene in automatico a cura del S.O. Vista schermata di Clock synchronization	C
Utilizzo di programmi di utilità privilegiati	8.18	E' presente una limitazione sull'uso di internet (web filtering) fornito direttamente dal provider dei servizi internet Non sono presenti blocchi specifici sulle porte USB.	OSS 2
Installazione di software su sistemi operativi	8.19	L'installazione di software è affidata esclusivamente a personale autorizzato con account amministratore.	
Sicurezza delle reti	8.20	POL-18 POLITICA DI RETE WIRELESS in Rev. 0 del 12-01-24	OSS 3
Sicurezza dei servizi di rete	8.21	POL-6 POLITICA DI CRITTOGRAFIA in Rev. 0 del 12-01-24	
Segregazione delle reti	8.22	Screen shot politiche di web filtering e regole del firewall	
Filtraggio Web	8.23		
Uso della crittografia	8.24		
Ciclo di vita dello sviluppo sicuro	8.25	N.A.	
Requisiti di sicurezza dell'applicazione	8.26		
Architettura di sistema sicura e principi ingegneristici	8.27		
Codifica sicura	8.28		
Test di sicurezza in fase di sviluppo e accettazione	8.29		
Sviluppo in outsourcing	8.30		
Separazione degli ambienti di sviluppo, test e produzione	8.31		
Gestione del cambiamento	8.32	PR 6.3_Gestione_del_Cambiamento	C
Informazioni sul test	8.33	MOD. 6.1.2.4 VULNERABILITY ASSESSMENT REPORT del 27-07-24	C
Protezione dei sistemi informativi durante i test di audit	8.34	MOD. 6.1.2.5 PENETRATION TEST REPORT del 15-09-24 DISASTER RECOVERY REPORT del 12-09-2024 POL-7 POLITICA DI BACKUP E RIPRISTINO DEI DATI in Rev. 0 del 12-01-24	

LEGENDA: **C** = conforme **NC** = non conforme **OSS** = osservazione

NOTE:

Data: 18/10/2024	Firma Auditor: <i>Teresa Battaglia</i>
------------------	--

RAPPORTO DI AUDIT			Rev 0 del 16-01-2024 Pag. 1 di 1
Rapporto n°1/2024		Data: 18/10/2024	
Processo / Funzione auditati: DIREZIONE – AMMINISTRATORE DI SISTEMA			
Persone intervistate: Dr. Italo Corvino – Ing. Ciro Esposito			
Argomenti esaminati: Ruoli e Responsabilità, Organigramma, nomine, ambiti di trattamento, istruzioni operative, formazione soggetti autorizzati al trattamento. Analisi dei rischi - DPIA e misure organizzative di mitigazione dei rischi, Informative agli interessati, Procedure data Breach, Policies aziendali, Misure tecniche di mitigazione dei rischi.			
TEAM DI VERIFICA ISPETTIVA			
Responsabile: Dott.ssa Teresa Battaglia Ispettori: Dott.ssa Teresa Battaglia / _____			
Osservatori: _____ / _____ / _____			
ESITO (*): POSITIVO CON RISERVA		ELEMENTI DI RISCOントRO (Vedi lista di riscontro allegata)	
(*) Positivo ; Positivo con riserva (vedere osservazioni); Negativo (necessità di AC)			
NC /Oss	Rif. normativo	Descrizione delle Non conformità (NC) e delle Osservazioni (Oss) riscontrate	
OSS1	5.30	Non è presente una rete mobile da utilizzare in assenza di rete fissa (di <i>Failover</i>) per garantire la continuità	
OSS2	8.18	Si raccomanda di bloccare l'utilizzo delle porte USB	
OSS3	8.20	Non è presente una rete wireless dedicata agli ospiti	
EVENTUALI PROVVEDIMENTI:			
Trattandosi di spunti di miglioramento, l'accoglimento degli stessi sarà verificato nel corso del prossimo audit.			

AC/AP	<input type="checkbox"/>	NO	<input type="checkbox"/>	SI n° _____ del _____	Firma Responsabile:
-------	--------------------------	----	--------------------------	-------------------------	---------------------

Firma Responsabile Team di Verifica:	Firma Responsabile attività verificata:
<i>Teresa Battaglia</i>	<i>Italo Corvino</i>
	<i>Ciro Esposito</i>