| Eurobottoni s.r.l. | Regolamento aziendale per la gestione delle informazioni riservate, per la privacy e per l'utilizzo dei sistemi informatici |
|---|---|

| N. | Contenuto | Riferimento normativo |
|---|---|---|
| 1. | **Premessa** | n.a. |
| 2. | **Strumenti di "controllo a distanza"** | Articolo 4 della legge 20 maggio 1970, n. 300<br>Art. 09 – 30 – 33- 34 – 35 -37 (679/16) |
| 3. | **Utilizzo degli apparati elettronici (fissi e mobili)** | Art. 04 – 05 – 25 – 32 |
| 4. | **Gestione delle Password** | Art. 25 - 32 |
| 5. | **Uso della rete e dei supporti magnetici** | Art. 25 - 32 |
| 6. | **Utilizzo dei telefoni, fax e fotocopiatrici aziendali** | Art. 04 – 05 – 25 – 32 |
| 7. | **Uso della rete internet e dei relativi servizi** | Art. 04 – 05 – 25 – 32 |
| 8. | **Protezione antivirus / anti intrusione / accessi** | Art. 04 – 05 – 25 – 32 |
| 9. | **Trattamento dei dati senza l'ausilio di strumenti elettronici (Cartaceo)** | Art. 25 - 32 |
| 10. | **Gestione del consenso** | Art. 07 |
| 11. | **Gestione delle informative** | Art. 12 -13 - 14 |
| 12. | **Gestione degli incarichi e delle autorizzazioni** | Art. 28 e 29 |
| 13. | **Gestione delle attività di marketing** | Art. 07 – 21 |
| 14. | **Riferimento alla linea guida su posta elettronica ed internet** | linea guida del Garante per posta elettronica e internet Gazzetta Ufficiale n. 58 del 10 marzo 2007 |
| 15. | **Applicazione delle misure relativa all'amministratore di sistema** | Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) |
| 16. | **Procedura di verifica del rispetto delle misure minime di sicurezza** | Art. 32 |
| 17. | **Osservanza delle disposizioni in materia di Protezione dei dati Personali** | Art. 32 |
| 18. | **Gestione dei dati personali particolari presenti in azienda elettronici e cartacei** | Art. 29 e Art. 32 |
| 19. | **Gestione dei dati dei dipendenti utilizzati nella attività lavorativa e loro accessibilità** | Art.21 e Art.32 |
| 20. | **Videosorveglianza** | Art. 32 e Provvedimenti a carattere generale - 08 aprile 2010 - art. 04 legge 1970 statuto dei lavoratori |
| 21. | **Gestione dei cookie presenti sul sito** | Art.13 e http://www.garanteprivacy.it/cookie |
| 22. | **Regole scrivania pulita, schermo in ordine** | Art. 32 |
| 23. | **Non osservanza della normativa** | Art. 83 e succ. |
| 24. | **Conservazione dei dati** | Art. 13 |
| 25. | **Destinatari di eventuali comunicazioni** | Art. 13 art. 28 |

| | | |
|---|---|---|
| **26.** | **Attuazione dei diritti dell'interessato** | Art. 15 - 21 |
| **27.** | **Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione** | Art. 22 |
| **28.** | **Privacy by design e by default** | Art. 25 |
| **29.** | **Registro dei trattamenti / censimento dati** | Art. 30 |
| **30.** | **Sicurezza del trattamento** | Art. 32 |
| **31.** | **Data breach** | Art. 33 e art. 34 |
| **32.** | **Valutazione impatto sulla protezione dei dati (PIA)** | Art. 35 e art. 36 |
| **33.** | **Responsabile protezione dei dati (DPO)** | Art. 37 – 39 |
| **34.** | **Codici di condotta e certificazioni** | Art. 40 – 43 |
| **35.** | **Trasferimento dei dati verso paesi terzi o organizzazioni internazionali** | Art. 44 - 49 |
| **36.** | **Segnalazione di problematiche / Aggiornamento e Revisione** | |
| **37.** | **Modifiche effettuate** | |
| **38.** | **Sanzioni pecuniarie** | |
| **39.** | **Aspetti di responsabilità civile** | |

| Eurobottoni s.r.l. | Regolamento aziendale per la gestione delle informazioni riservate, per la privacy e per l'utilizzo dei sistemi informatici |
|---|---|

**1. Premessa**

La progressiva diffusione delle nuove tecnologie informatiche, l'accesso in mobilità, fuori dal luogo di lavoro, ed in particolare il libero accesso alla rete Internet da Personal Computer, tablet, smartphone espone ogni attività lavorativa, ai rischi informatici con un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine della stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche devono sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, i responsabili hanno adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Il rispetto del presente regolamento deve essere garantito da parte di tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché di tutti i collaboratori, a prescindere dal rapporto contrattuale con essa intrattenuto (lavoratori somministrati, collaboratori, in stage, ecc.).

Nel proseguo del presente regolamento, coloro che sono tenuti al rispetto delle sue disposizioni vengono denominati, nel loro complesso, come il "personale".

Il nuovo regolamento Europeo sul trattamento dei dati personali (679/16) stabilisce come sua base fondante la "accountability" (responsabilità del risultato perseguito). Cioè la responsabilizzazione del titolare del trattamento in merito a tutta la applicazione del suddetto regolamento europeo, e non più nella mera applicazione di alcune misure minime di sicurezza. Questo si esplicita una dettagliata analisi inziale ed in una valutazione periodica delle attività e di tutte le novità che potranno emergere in modo da poter sempre dimostrare che ogni processo aziendale sia sempre visto anche nell'ottica della sicurezza dei dati personali.

Il presente regolamento e tutti gli allegati che esso richiamo seguono questa ottica di responsabilità e di analisi.

Eurobottoni s.r.l. si compone al momento di due soci, non ci sono dipendenti e non ci sono agenti.

**2. Strumenti di "controllo a distanza dei lavoratori"**

*"Articolo 4 della legge 20 maggio 1970, n. 300 (Impianti audiovisivi e altri strumenti di controllo).*

*1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.*

*2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*

*3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal vigente regolamento sulla privacy."*

La tecnologia ha dotato le aziende di una gran quantità di apparati elettronici mobili con un sempre maggior numero di funzioni. L'azienda non utilizza strumenti assimilabili a quelli indicati nell'art. 4 dello statuto dei lavoratori (modificato dal Dlgs 151/2015) in quanto non ha dipendenti.

**3. Utilizzo degli apparati elettronici (client / notebook, tablet, smartphone).**

Lo strumento informatico e tutti gli apparati elettronici sono strumenti di lavoro devono essere custoditi con cura evitando ogni possibile forma di danneggiamento. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

In particolare si deve porre particolare attenzione con tutti quelli strumenti contenenti dati aziendali utilizzati fuori dall'ambiente lavorativo, a rischio smarrimento e furto.
In Eurobottoni vengono utilizzati tre pc dai due soci
Tutti e tre i pc sono protetti da pw, antivirus e firewall
Il backup viene effettuato soltanto del programma di contabilità. Su chiavetta esterna.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Titolare nel caso in cui siano rilevati virus ed adottando quanto previsto nelle presenti Linee Guida relative alle procedure di protezione antivirus.
Svuotare quotidianamente il "cestino" di windows od analoghi.
Nel caso di portatili utilizzati esternamente alla struttura, il pc sarà protetto da user e password (anche uguale a quello fisso in sede), avrà antivirus, e tutto il software aggiornato; l'utilizzatore è incaricato quale responsabile del pc e dei dati al momento dell'utilizzo di tale strumento esternamente alla struttura.

**4. Gestione delle Password**
La password per l'accesso al proprio pc devono essere di almeno otto caratteri, non facilmente riconducibile all'utente;
Le password utilizzate hanno una durata massima di 360 giorni, passati i quali il sistema richiede il cambiamento;
Le password modificate non possono essere uguali alle tre precedenti inserite dall'utente;
Le credenziali non utilizzate per almeno sei mesi, o in caso di perdita della qualità dell'incaricato stesso, devono essere disattivate.
Non è necessario il salvataggio delle password.

**5. Utilizzo della rete intranet e dei supporti magnetici e ottici.**
Si raccomanda di tenere in altra posizione / luogo / sede il supporto di backup utilizzato
Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.
Non è consentito scaricare files contenuti in supporti magnetici/ ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
Tutti i files di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo da parte dell'incaricato.

**6. Utilizzo dei telefoni, fax e fotocopiatrici aziendali**
Non sono necessarie regole di utilizzo in quanto non ci sono dipendenti

**7. Uso della rete Internet e dei relativi servizi**
Le regole sotto indicate sono buone regole, ovviamente da applicare con attenzione a dipendenti, collaboratori e subordinati, non così dirette per il titolare del trattamento che ha necessità di gestione più ampia
L'accesso ad internet avviene dal router.
Il Personal Computer abilitati alla navigazione in Internet costituisce uno strumento della società necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
E' rischioso lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, la partecipazione a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

In caso di invio di una e-mail a più destinatari, inviarla a sé stessi ed in CCN (copia nascosta) a tutti gli altri destinatari, in modo che non vengano diffusi gli indirizzi e-mail tra i diversi destinatari della comunicazione.
Nell'invio della posta elettronica, va inserita la seguente o comunque affine dicitura:
*"Questo indirizzo di posta elettronica è di proprietà del titolare del trattamento. I messaggi in trasmissione ed in ricezione si presumono di attinenza e competenza prettamente aziendale; essi possono essere letti, gestiti e/o condivisi anche oltre la sfera personale dell'assegnatario del presente indirizzo. Le informazioni contenute nella presente comunicazione e nei relativi allegati possono essere riservate e sono, comunque, destinate esclusivamente alla Società alla quale appartiene l'indirizzo di destino. La comunicazione, la diffusione, la copiatura dei contenuti della presente comunicazione e dei documenti allegati da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 del Codice penale che ai sensi del regolamento europeo 679/16. Qualora abbiate ricevuto questa comunicazione per errore, vi preghiamo di distruggerla e di informare immediatamente il mittente"*

**8. Protezione antivirus / anti intrusione / accessi**
L'accesso dall'esterno e verso l'esterno della rete avviene attraverso il router, che permette l'accesso singolarmente da parte di tutte le postazioni.
I pc hanno firewall e antivirus costantemente aggiornati.
Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico della società mediante virus o mediante ogni altro software aggressivo.
Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.
Non è consentito l'utilizzo di memorie esterne di ogni genere di provenienza ignota.
Limitare la trasmissione di files eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computers in rete.
I PC devono essere costantemente sottoposti a controllo anti-virus.
Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
a) sospendere ogni elaborazione in corso senza spegnere il computer;
b) segnalare l'accaduto al tecnico esterno.
l software antivirus e anti intrusione sono sottoposti a costante e frequente aggiornamento, in automatico, o giornaliero da parte degli incaricati.
L'accesso fisico alla struttura è protetto dal portone di accesso.

**9. Trattamento dei dati senza l'ausilio di strumenti elettronici (Cartaceo)**
Il titolare si occupa della stampa, della gestione e dell'archiviazione di tutti i documenti necessari,
I documenti cartacei sono custoditi tutti nella struttura, l'accesso alla struttura è protetto dalla porta, e/o dalla presenza del personale. Tutti i documenti cartacei contenenti dati personali dovranno essere trattati con cautela, non dovranno essere lasciati incustoditi, leggibili sulle scrivanie degli incaricati in presenza di persone esterne, trattati da persone non autorizzate, e quando distrutti non dovrà essere possibile una loro rilettura.
Non ci sono dati personali particolari in quanto le attività svolte non prevedono il loro trattamento, ne, al momento, ci sono dipendenti.

**10. Gestione del consenso**
Il trattamento dei dati di clienti e di fornitori a fini esclusivamente amministrativo contabili viene escluso dalla necessità del consenso preventivo dell'interessato.
Non ci sono trattamenti di dati personali che necessitano di consenso

**11. Gestione delle informative**
Le informative vengono gestite nel seguente modo:
inviate a clienti e fornitori al momento dell'inizio del trattamento tramite il sito internet, oltre a quella dei cookie.

**12. Gestione degli incarichi e delle autorizzazioni, ed aggiornamenti dei profili di autorizzazione**

Al momento non ci sono dipendenti quindi non necessitano incarichi.
Le autorizzazioni vengono gestite nel seguente modo: Vengono autorizzate figure esterne, quali commercialista, e consulenti vari, all'accesso ai dati personali di cui è titolare la società ed al loro trattamento nelle modalità e nella quantità in cui questo è necessario al corretto svolgimento del lavoro richiesto. L'accesso può essere on site, oppure il trattamento può avvenire nella sede della figura autorizzata, in ogni caso quest'ultima è autorizzata e nominata responsabile esterno del trattamento e per quel determinato periodo nel quale tratta i dati e per le mansioni da essa svolte (sia internamente che esternamente), il titolare rimane in ogni caso eurobottoni s.r.l. stessa.

**13. Gestione delle attività di marketing aziendale.**

La società non effettua attività di marketing aziendale.

**14. Riferimento alla linea guida su posta elettronica ed internet**

In merito alla linea guida emessa dal garante in data 01/03/07 concernente posta elettronica ed internet sul posto di lavoro, ed al relativo trattamento dei dati dei dipendenti, che qui riportiamo quale rimando per una più corretta gestione del sistema, e per individuare le nostre azioni intraprese all'applicazione della stessa.

***……"TUTTO CIÒ PREMESSO IL GARANTE***

*1) prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;*

*2) indica inoltre, ai medesimi datori di lavoro, le seguenti linee guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:*

*a) l'adozione e la pubblicizzazione di un disciplinare interno (punto 3.2.);*

*b) l'adozione di misure di tipo organizzativo (punto 5.2.) affinché, segnatamente:*

- *si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;*
- *si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;*
- *si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;*

*c) l'adozione di misure di tipo tecnologico, e segnatamente:*

*I. rispetto alla "navigazione" in Internet (punto 5.2., a):*

- *l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;*
- *la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;*
- *il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;*
- *l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;*
- *la graduazione dei controlli (punto 6.1.);*

*II. rispetto all'utilizzo della posta elettronica (punto 5.2., b):*

- *la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;*
- *l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;*
- *la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;*

- *consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;*
- *l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;*
- *la graduazione dei controlli (punto 6.1.);*

*3) vieta ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori (punto 4), svolti in particolare mediante:*
*a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;*
*b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;*
*c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;*
*d) l'analisi occulta di computer portatili affidati in uso; "…….*
Il provvedimento non è applicabile in quanto non ci sono, al momento dipendenti.

**15. Applicazione delle misure relativa all'amministratore di sistema (G.U. n. 300 del 24 dicembre 2008).**
Con il provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)" il garante ha voluto andare ad inquadrare la figura dell'amministratore di sistema, sottoponendo a tutti i titolari del trattamento dei dati la necessità di un maggior controllo sul lavoro svolto da tal specialisti, forse sottovalutato nell'importanza che riveste per la sicurezza dei dati e non solo all'interno di moltissime organizzazioni.
Nello studio, dopo una attenta valutazione e consultazione tra il titolare del trattamento, il consulente esterno, la società esterna di hardware e software e il personale che internamente si occupa delle pratiche amministrative si è deciso di poter rientrare nei casi che il garante ha escluso dall'obbligo di adempimento del provvedimento suddetto, andando ad individuare due motivi fondamentali:

1- L'organizzazione è di piccolissime dimensione ed anche l'apparato informatico non è molto complesso: le attività di normale manutenzione e controllo del sistema informatico sono gestite da personale interno già autorizzato, per le attività di manutenzione straordinaria l'azienda si affida a due professionisti esterni specializzata, sia per l'hardware che per il software (vedi Faq 1 del provvedimento), tali sistemisti sono stati debitamente incaricati e non hanno una manutenzione ad ore, ma sono a chiamata (e quindi non sono inquadrabili come amministratori di sistema).
2- Il trattamento dei dati in formato elettronico non prevede dati particolari.

**16. Procedura di verifica del rispetto delle misure minime di sicurezza**
Ogni anno insieme alla revisione periodica dei documenti viene effettuata una piccola verifica ispettiva interna, sulle misure minime di sicurezza e sui principali obblighi previsti dalla legge; vedi allegato 09 per il dettaglio.

**17. Osservanza delle disposizioni in materia di Protezione dei dati Personali**
E' obbligatorio attenersi alle disposizioni in materia di Privacy e delle misure di sicurezza, come indicate nella lettera di individuazione di incaricato del trattamento dei dati nel rispetto del presente regolamento interno e degli articoli del regolamento europeo indicanti i requisiti di sicurezza (art.32).

**18. Gestione dei dati personali particolari presenti in azienda elettronici e cartacei**
Gli unici dati particolari "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" sono quelli relativi al personale dipendente dell'organizzazione trattati per la gestione del rapporto lavorativo. Non ci sono al momento dipendenti.

**19. Gestione dei dati dei dipendenti utilizzati nella attività lavorativa e loro accessibilità**
**19.1 Assunzione:**
**19.2 Cessazione del rapporto di lavoro:**
al momento non sono presenti dipendenti

**19.3 manutenzione della infrastruttura informatica**
Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dei professionisti o dei responsabili IT esterni accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

**20. Gestione della Video Sorveglianza**
E' presente una sola videocamera a esclusivo uso di video citofono.

**21. Gestione dei cookie presenti sul sito**
E' presente un sito internet con cookie policy e privacy policy

**22. Regole scrivania pulita, schermo in ordine**
Si ricorda di mantenere:

- la propria scrivania ed il proprio ufficio "pulito", prestando particolare attenzione a tutte le informazioni relative ai dati personali di cui è titolare la società e quelle riservate relative ad informazioni aziendali da non diffondere.
- la propria scrivania virtuale (desktop del pc) "pulita" prestando particolare attenzione a tutte le informazioni importanti (da non tenere sul desktop, in quanto a rischio di cancellazione, perdita, accesso non autorizzato).

**23. Non osservanza della normativa**
Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento sono perseguibili con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

**24. Conservazione dei dati**
Come individuato nel censimento dei data base e dei dati personali presenti in azienda (allegato 11); sono indicate le tempistiche di conservazione dei dati; per obblighi legislativi abbiamo:

- i 10 anni per tutti i documenti amministrativo contabili dei clienti e dei fornitori (contratti, fatture, ddt, ecc) (in formato elettronico e cartaceo);
- circa 1 mese per il backup (in formato elettronico);

**25. Destinatari di eventuali comunicazioni**
Sotto indicati i destinatari di eventuali comunicazioni; tralasciando gli enti pubblici e giudiziari, le persone fisiche e giuridiche esterne che hanno accesso o alle quali sono comunicati i dati sono:

- Avvocato;
- Commercialista;
- Tecnici informatici;

**26. Attuazione dei diritti dell'interessato**

A seguito degli articoli da 15 a 22 del regolamento europeo l'azienda ha predisposto un modulo standard "allegato 12" al presente regolamento interno, per poter rispondere agli interessati al trattamento che facciano richiesta di tutela dei propri diritti. E viene utilizzato il presente regolamento come procedura di riferimento per la gestione di tali richieste.
La corretta gestione di una richiesta dell'interessato parte dalla ricerca dei suoi dati personali presso la sede del titolare del trattamento e presso tutti gli eventuali responsabili ai quali è stato comunicato; questa attività deve iniziare con la consultazione del registro dei trattamenti, che è dove sono indicati tutti i dati trattati dall'azienda, con le relative specifiche (finalità, tempistiche, tipologia, ecc, ecc).
Valutato quindi in quali di questi database sono presenti i dati dell'interessato, e a quali esterni sono stati eventualmente comunicati si risponde alle sue richieste; e contestualmente si mettono in pratica andando ad attuarle sui database individuati.
In particolare

- **Articolo 15 - diritti di accesso dell'interessato**, l'interessato ha diritto di conoscere:
  L'esistenza o meno di un trattamento presso il titolare del trattamento al quale ha fatto richiesta, e se affermativa:
  Le finalità del trattamento;
  Le categorie dei dati trattati;
  I destinatari ai quali i dati sono stati comunicati;
  Il periodo di conservazione;
  L'origine dei dati, se non raccolti dal titolare in oggetto;
  L'esistenza di un processo automatico di profilazione;
  Le garanzie nel caso di trasferimento dati extra ue;
- **Articolo 16 - diritto di rettifica**, l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo, ecc, ecc.
- **Articolo 17 - diritto alla cancellazione "diritto all'oblio",** L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti (si veda nel dettaglio l'articolo del regolamento europeo).
  2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
- **Art.18 – diritto alla limitazione**, L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi: omissis (si veda nel dettaglio l'articolo suddetto del regolamento europeo)
  2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
  3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.
- **Articolo 19 - Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento**; il titolare deve notificare alle altre organizzazioni alle quali ha comunicato i dati personali le richieste dell'interessato, queste comunicazioni, sono fatte singolarmente per ogni articolo sopra elencato, nel documento apposito "allegato 12".
- **Articolo 20 - Diritto alla portabilità dei dati (C68)**, L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del

titolare del trattamento cui li ha forniti qualora: omissis (si veda nel dettaglio l'articolo suddetto del regolamento europeo);
2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui

- **Articolo 21 - Diritto di opposizione:** L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

**27. Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione**

Eurobottoni s.r.l. non effettua attività di profilazione automatizzata.

**28. Privacy by design e by default**

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

**28.1 privacy by design**

Le attività oggetto del presente regolamento non prevedono lo sviluppo di prodotto e/o servizi che hanno impatto sulla privacy degli utenti

**28.2 privacy by default**

Le attività in merito al trattamento dei dati personali delle persone fisiche e più in generale di tutti i dati presenti all'interno dello studio sono oggetto di continua valutazione e attenzione da parte della direzione e di tutti gli utenti interni ed esterni. Tutta la struttura del presente documento e tutti i documenti allegati allo stesso, così come i controlli costanti previsti sono evidenza della impostazione predefinita di tutto il sistema alla privacy ed alla sicurezza dei dati in generale.

**29. Registro dei trattamenti / censimento dati**

Non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

**30. Sicurezza del trattamento**

Tutte le misure di sicurezza previste per tutti i trattamenti sui dati personali, su qualunque supporto, presenti in azienda sono definite e spiegate nel presente regolamento. Lo stesso è condiviso con tutti i responsabili e gli incaricati al trattamento e estrapolato nel documento di incarico dato all'assunzione.
Esso è revisionato periodicamente ed ogni volta che ce ne sia bisogno.
Si riporta quanto all'articolo 32 come spunto per tutta la gestione della sicurezza dei dati:
misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

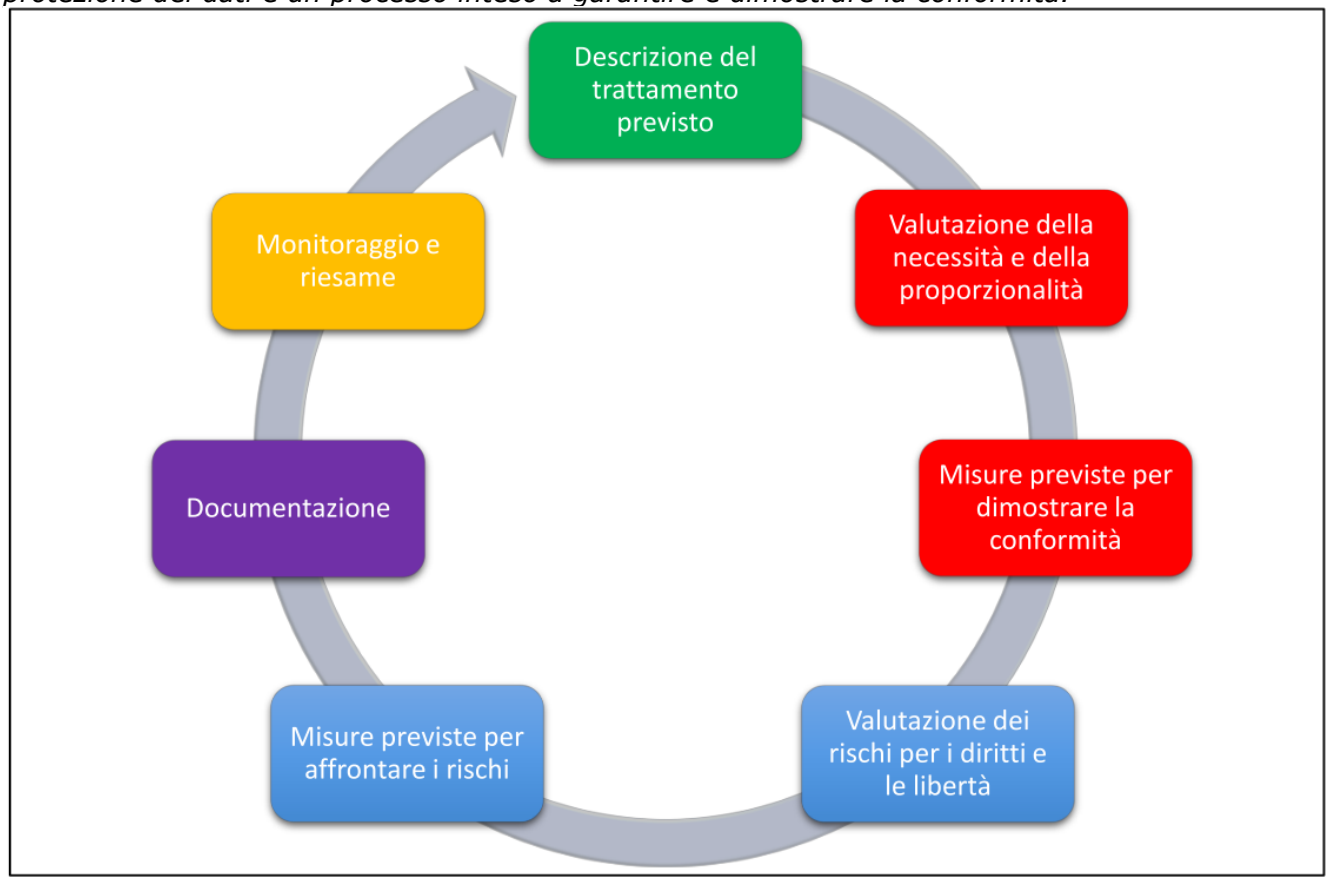
**31. Data breach**

Al momento della scoperta della violazione si deve redigere uno dei due allegati per valutare il rischio generato dalla violazione, le misure prese, i dati oggetto della violazione, ecc, ecc. in modo tale da valutare la necessità o meno della comunicazione al garante, od in caso di rischio elevato, anche agli interessati.
Il titolare del trattamento ha valutato che nessun dato presente all'interno della propria struttura, nel caso di una violazione, può generare un rischio per i diritti e per le libertà degli interessati

**32. Valutazione impatto sulla protezione dei dati (DPIA)**

La Dpia è lo strumento principale per dimostra il processo di accountability nei confronti del sistema di gestione dei dati personali.
Non è uno strumento obbligatorio; lo risulta quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali; in particolare:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico
Al fine di supportare il titolare del trattamento a compiere queste scelte, le Linee Guide del WP 29 forniscono nove criteri di riferimento per capire quando, con molta probabilità, sarà necessario procedere alla DPIA:
1. Trattamenti che comportano valutazioni della persona e profilazione (es. rendimento professionale, situazione economica, ubicazione, spostamenti, ecc);
2. Decisioni automatizzate con effetti giuridici significativi (es. esclusione da benefici);
3. Attività di monitoraggio sistematico (es. raccolti di dati attraverso reti, sorveglianza sistematica in un'area accessibile al pubblico);
4. Dati sensibili o dati di natura estremamente personale (es. opinione politiche o sindacali, condanne penali, cartelle cliniche, ecc.)
5. Trattamenti di dati su larga scala (il concetto di larga scala va riverito a: numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di

riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata, o persistenza, dell'attività di trattamento; ambito geografico dell'attività di trattamento);
6. Combinazione o raffronto di insiemi di dati (es. dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti);
7. Dati relativi a interessati vulnerabili (si va dai minori sino ai soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti);
8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici);
9. In generale, infine, tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es. lo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento).
Eurobottoni s.r.l. non effettua nessun trattamento tra tipologie individuate dal regolamento europeo (i punti a, b, c) ne dalle specifiche della linea guida del gruppo WP29.
Infatti analizzando il registro dei trattamenti (allegato 11) si evince che tutte le finalità elencate nel registro stesso non rientrano nelle tipologie sopra indicate.
*"Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali4, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24)5. In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità."*




**32.1 consultazione preventiva**

Non avendo mai effettuato una dpia, la organizzazione non ha nemmeno mai effettuato una consultazione preventiva al garante

**33. Responsabile protezione dei dati (DPO)**
Eurobottoni s..rl. NON ha designato un responsabile della protezione dei dati perché:
- NON è un'autorità pubblica o da un organismo pubblico;
- le attività principali del titolare NON consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
- le attività principali del titolare NON consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

**34. Codici di condotta e certificazioni**
Non sono previsti al momento codici di condotta da parte della nostra associazione di categoria con finalità simili

**35. Trasferimento dei dati verso paesi terzi o organizzazioni internazionali**
Tutti i dati personali trattati da Eurobottoni sono gestiti all'interno della Comunità Europea.

**36. Segnalazione di problematiche / Aggiornamento e revisione**
E' consigliabile aggiornare con cadenza annuale le presenti Linee Guida.

**37. Modifiche effettuate**
Rev. 01 ;
Rev. 02 ;
Rev. 03 ;

**Regime Sanzionatorio**
Secondo l'art.58 paragrafo 2 comma i) è potere del garante della privacy infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso.
Inoltre secondo l'art. 82, chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

**38. Sanzioni pecuniarie**
L'articolo 83 al paragrafo 2 stabilisce come fissare l'ammontare della sanzione; il successivo paragrafo 4 stabilisce quali violazioni sanzionare col massimo di 10 milioni di euro od il 2% di fatturato globale se superiore, mentre il paragrafo 4 stabilisce quali violazioni sanzionare col massimo di 20 milioni di euro od il 4% di fatturato globale se superiore.

**39. Aspetti di responsabilità civile**
**Art. 2050 c.c.**
E ' prevista pertanto una inversione dell'onere della prova nell'azione risarcitoria ex articolo 2043 c.c.: l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire la sicurezza dei dati detenuti.
A livello pratico questo significa che l'azienda, il professionista, la PA ecc., per evitare ogni responsabilità deve dimostrare di aver adottato "tutte le misure idonee ad evitare il danno", e quindi di aver messo in essere tutte le misure di sicurezza al meglio possibile (la miglior tecnologia disponibile). Il che non è affatto facile da dimostrare...
**Art. 2049 c.c.**
In generale poi a carico dell'azienda risulta comunque la responsabilità ex art. 2049 c.c., ovvero la responsabilità prevista in capo a padroni e committenti.

L'art. 2049 difatti recita: "padroni e committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze cui sono adibiti".

**Legge n. 547/1993**

*Crimini informatici commessi da dipendenti ed addebitabili all'azienda.*

La legge 547/93 ha introdotto nel nostro ordinamento vari "crimini informatici", ovvero l'attentato a impianti informatici di pubblica utilità, falsificazione di documenti informatici, accesso abusivo ad un sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, violazione di corrispondenza telematica, intercettazione di e-mail, danneggiamento di sistemi informatici o telematici (...).

Il datore di lavoro rischia di essere ritenuto in concorso con il dipendente a lui subordinato che ha commesso il crimine informatico, per non aver posto in essere tutte le misure di prevenzione e controllo idonee a garantire la sicurezza del trattamento dei dati.

La mancata adozione di tutte le misure idonee a ridurre al minimo i rischi viene considerata difatti un'agevolazione alla commissione del crimine.

**Eurobottoni s.r.l.**
(Titolare del trattamento)