# DOCUMENTO PROGRAMMATICO sulla SICUREZZA

# ai sensi del D.Lgs. 196/03 e del Regolamento UE n. 2016/679

| Stesura | Data | Firma |
|---|---|---|
| Redatto da : Daniele Peressutti | 25/05/18 | |
| Verificato da : Elio Pantanali | 25/05/18 | |
| Approvato da : Elio Pantanali | 25/05/18 | |

| Rev. n° | Oggetto della revisione | Data |
|---|---|---|
| 1.0 | Prima Emissione | 25/05/18 |
| 2.0 | Revisione Annuale | 31/03/19 |
| 3.0 | Revisione Annuale | 31/03/20 |
| | | |
| | | |
| | | |

| Distribuzione | Originale presso |
|---|---|
| GENERALE | Responsabile Direzione SI |

## INDICE

## Introduzione

Il 1 gennaio 2004 è entrato in vigore il D.Lgs. 30 giugno 2003, n° 196 "Codice in materia di protezione dei dati personali", nel seguito denominato brevemente "Codice" e successivamente il 25 maggio 2018 il Regolamento UE n. 2016/679 (di seguito "GDPR 2016/679").

Il Codice ed il GDPR 2016/679 prevedono che chiunque tratti, in nome proprio o conto terzi, dati personali sensibili con strumenti informatici, debba redigere, e aggiornare almeno annualmente, un Documento Programmatico sulla Sicurezza (DPS).

Quello che segue è il DPS relativo alla protezione dei dati personali che la Marcegaglia Palini & Bertoli tratta sia come titolare, sia come responsabile.

Questo documento, nella sua versione più aggiornata, viene pubblicato sulla intranet aziendale di Marcegaglia Palini & Bertoli all'indirizzo http ://intranet.ITA.evraz.com/ a disposizione di tutto il personale.

## Elenco dei trattamenti dei dati personali

I dati personali trattati, o in via di trattamento, da parte della Marcegaglia Palini & Bertoli, possono essere ricondotti alle seguenti tipologie :

- Dipendenti e collaboratori;
- Clienti;
- Fornitori;
- Frequentatori web;
- Utenti servizi web.

### *Trattamenti dei dati di dipendenti e collaboratori*

Soggetti

Sono coloro che hanno in essere un rapporto di lavoro subordinato o di collaborazione con la Marcegaglia Palini & Bertoli.

Finalità

Sono connesse al :
- trattamento giuridico ed economico del personale (e dei collaboratori) come il calcolo e pagamento della retribuzione, l'applicazione della normativa previdenziale e assistenziale, il rispetto degli adempimenti fiscali e contabili;
- selezione, reclutamento, valutazione del personale.

Ambito di diffusione e comunicazione

Questa tipologia di dati è soggetta alla comunicazione ad altri enti prefigurati per obblighi di legge.

Inoltre possono essere comunicati :
- ai sindacati, per l'espletamento dei conteggi relativi alle trattenute per l'iscrizione;
- alle banche, per l'espletamento delle pratiche di versamento delle competenze maturate.

### *Trattamenti dei dati di Clienti*

Soggetti

Appartengono alla tipologia dei Clienti :
- Soggetti che acquistano prodotti Marcegaglia Palini & Bertoli.

Finalità

Sono connesse alla :
- gestione della clientela : amministrazione, gestione ordini, contratti, spedizione e fatturazione, controllo dell'affidabilità e solvibilità;
- gestione del contenzioso.

Ambito di diffusione e comunicazione

I dati possono venire comunicati a terzi per obblighi assunti in fase contrattuale (ad es. istituti bancari).

### *Trattamento dei dati di Fornitori*

Soggetti

Fornitori di servizi relativi al processo produttivo, fornitori di servizi, anche in outsourcing.

Finalità

Connesse alla gestione dei fornitori : amministrazione, gestione ordini, contratti, arrivi e fatturazione.

Ambito di diffusione e comunicazione

I dati possono venire comunicati a terzi per obblighi assunti in fase contrattuale (ad es. istituti bancari).

### *Trattamento dei dati dei frequentatori web*

Soggetti

Sono rappresentati da qualsiasi persona che si collega al sito www.evrazpaliniebertoli.it, senza lasciare dati personali per nessun motivo, non si individuano quindi trattamenti.

Sono rilevanti ai fini privacy solo in termini sicurezza rispetto alla possibilità di accedere al sistema di Marcegaglia Palini & Bertoli.

Finalità

Eventuali analisi statistiche sulla modalità di navigazione all'interno del sito Marcegaglia Palini & Bertoli.

Ambito di diffusione e comunicazione

Sono dati che non vengono comunicati.

### *Trattamento dei dati degli Utenti di servizi web*

Soggetti

Sono rappresentati da persone che si collegano ai servizi offerti, tipo la sezione Area Riservata o la richiesta di informazioni.

Prevedono comunque la raccolta di dati, direttamente dall'interessato, e sono soggetti a tutela della privacy.

Finalità

Fasi precontrattuali in genere (invio propri dati personali al fine di ottenere informazioni commerciali o di altro genere).

Ambito di diffusione e comunicazione

Marcegaglia Palini & Bertoli può comunicare o indirizzare a specifici uffici particolari richieste ricevute via e-mail, perché è stata fornita una corretta informativa al riguardo.

Non sono previste comunicazioni di questi dati all'esterno della Marcegaglia Palini & Bertoli.

## Organizzazione preposta al trattamento dei dati personali

### *Titolare*

E' l'azienda Marcegaglia Palini & Bertoli nel suo complesso. Fisicamente i titolari sono i legali rappresentanti delle singole società.

### *Responsabile del trattamento*

E' il soggetto persona fisica preposto al trattamento dei dati personali.

Nella Marcegaglia Palini & Bertoli è stata individuata una tipologia di Responsabile :

- Responsabili interni. Sono persone fisiche, facenti parte della società, nominati dai rispettivi titolari;

Tra i responsabili interni si individuano due tipologie che differiscono tra loro per l'ambito di responsabilità :

- Responsabile aree omogenee. Si occupa dei trattamenti di aree omogenee per la società o per parte di essa. Sono nominati due responsabili a livello di gruppo : Area personale; Area Clienti e Fornitori.
- Responsabile sicurezza privacy. Si occupa della gestione del sistema informativo della Marcegaglia Palini & Bertoli. E' un unico responsabile, che garantisce il presidio della sicurezza e il rispetto delle norme.

L'elenco dei Responsabili è tenuto aggiornato e pubblicato sulla intranet aziendale di Marcegaglia Palini & Bertoli all'indirizzo http ://intranet.ITA.evraz.com/ a disposizione di tutto il personale.

### *Amministratori di sistema*

Sono persone fisiche che condividono la responsabilità di sovraintendere alla corretta funzionalità del sistema informativo di Marcegaglia Palini & Bertoli. Agiscono in base alle responsabilità delegate dal Responsabile sicurezza privacy, anche per quanto riguarda la sicurezza dei sistemi e dei dati.

L'elenco degli Amministratori è tenuto aggiornato e pubblicato sulla intranet aziendale di Marcegaglia Palini & Bertoli all'indirizzo http ://intranet.ITA.evraz.com/ a disposizione di tutto il personale.

### *Incaricati dei trattamenti*

Il ruolo di incaricato è ricoperto dalle persone fisiche che accedono ed elaborano i dati personali di cui Marcegaglia Palini & Bertoli è titolare o nominata responsabile.

Sono stati nominati incaricati i dipendenti/collaboratori che nel corso della loro attività accedono ai dati e li trattano, sia quelli di cui Marcegaglia Palini & Bertoli è titolare sia quelli di cui Marcegaglia Palini & Bertoli è responsabile per designazione da altri titolari.

## Analisi di rischio del sistema di elaborazione dei trattamenti

L'accesso alla rete Marcegaglia Palini & Bertoli da un qualunque client interno, residente su un PC con sistema operativo Windows, connesso alla rete stessa, è possibile con l'inserimento dello userID e della relativa password.

Senza ulteriori autorizzazioni, l'utente accede esclusivamente alla rete e agli host connessi, senza peraltro poter "entrare" sui vari server, ma riuscendo a "vedere" tutte le risorse di rete.

Gli utenti sono suddivisi in gruppi operativi, ciascuno dei quali può accedere ad alcune risorse e non ad altre. Questa suddivisione consente di impedire l'accesso a determinate risorse da parte di gruppi di utenti non abilitati e risulta più a prova di errore.

Ad esclusione di alcuni server, agli utenti non è comunque consentito un accesso diretto ai dati. L'accesso è sempre mediato da un'applicazione cui l'utente può, o non può, avere accesso.

### *Descrizione della rete*

La descrizione della rete, i dettagli delle connessioni e delle autorizzazioni sono contenuti nel documento riservato ANALISI DEL RISCHIO DELLA RETE MARCEGAGLIA PALINI & BERTOLI.

## Protezione fisica dei sistemi

Tutti i sistemi centralizzati contenenti dati personali o strategici sono segregati fisicamente e protetti da un sistema automatico antincendio.
Tutti i sistemi risiedono nella stessa località al piano seminterrato della palazzina uffici e possono essere soggetti a fenomeni tellurici e di inondazione.

Il rischio tellurico è considerato non elevato a San Giorgio di Nogaro e di impatto limitato dall'ubicazione. Più probabile il rischio inondazione, peraltro già manifestato (essendo l'ubicazione sotto falda).

Marcegaglia Palini & Bertoli ritiene i due rischi accettabili, e sufficiente la protezione offerta dal sistema antincendio. Non esiste quindi una procedura di ripristino, nel caso dovesse verificarsi uno di questi eventi accidentali, ma ne verrà studiata una al momento.

L'accesso all'area dei sistemi è informale e posto sotto il controllo degli addetti. Fuori orario di lavoro il sito è chiuso a chiave ed allarmato.

L'area non è soggetta a sorveglianza notturna e fuori orario di lavoro.

Eventuali incidenti della sicurezza fisica sono subito segnalati al Responsabile sicurezza privacy.

## Protezione logica dei dati

Il controllo degli accessi ai dati è suddiviso sui seguenti livelli

### *Livello rete*

L'accesso alla rete Marcegaglia Palini & Bertoli è consentito dall'interno attraverso l'immissione di userID e password validi da parte dell'utente.

Questo livello consente di visualizzare tutti i nodi della rete, senza poter eseguire nessuna operazione, escluso quelle relative a directory dichiarate accessibili.

### *Livello applicazioni*

L'accesso diretto ai dati contenuti in alcuni server non è consentito agli utenti. L'accesso è mediato da una o più applicazioni che consentono, agli utenti appartenenti a determinati gruppi, di operare. Alcune applicazioni per essere attivate implicano l'immissione da parte dell'utente di ulteriori credenziali (userID e password).

L'utente è in grado di interagire con tutte le applicazioni consentite dal suo livello di autorizzazione, ma non è in grado di modificarle o di modificare le impostazioni di nessun sistema.

L'addetto, d'intesa con l'Amministratore di sistema, può cambiare le impostazioni esistenti, ivi compresi i profili di autorizzazione dei singoli utenti o dei gruppi di utenti.

### *Livello massimo*

Questo livello è riservato agli addetti appartenenti alla Direzione SI per lo svolgimento dei propri compiti operativi.

Il cambiamento delle impostazioni esistenti è consentito solo agli Amministratori di sistema.

### *Mantenimento dell'integrità e della riservatezza*

I dischi di sistema contenenti dati personali o strategici lavorano in modalità ridondata RAID 1 (per i server host fisici) con disco di hot spare e RAID 5 (per la SAN ospitante le macchine virtuali).

Non esistono ulteriori meccanismi, esterni alle applicazioni, deputati al controllo dinamico dell'integrità dei dati. I dati sono soggetti giornalmente ad operazioni di backup, non verificate, che offrono una ridondanza intrinseca.

Gli utenti accedono solo ai dati a cui i loro profili di autorizzazione consentono di accedere. Gli accessi ad Internet sono registrati su un log di sistema.

Gli addetti accedono ai sistemi contenenti dati a criticità elevata con autorizzazione a livello amministratore. Ciò comporta, da parte loro, una maggiore responsabilità e attenzione sulle loro azioni. Gli accessi di questo tipo sono registrati su un log di sistema non modificabile.

### *Rilevazione degli incidenti di sicurezza*

Chiunque rilevi (o supponga di rilevare) un incidente della sicurezza fisica (manomissione di apparati o ambienti) o logica (malfunzionamenti o accessi indebiti alle applicazioni o ai dati) sospende immediatamente la propria operatività e ne dà immediato avviso a un addetto o all'amministratore di sistema o al Responsabile sicurezza privacy (EMail : DG_ITA_SystemAdmins@evraz.com).

Marcegaglia Palini & Bertoli non ritiene indispensabile l'adozione di un piano per la gestione degli incidenti della sicurezza, e conseguentemente l'adozione di procedure sistematiche per l'archiviazione e l'analisi degli stessi

Il Responsabile sicurezza privacy, con l'Amministratore di sistema, definisce, caso per caso, la procedura da adottare per la classificazione dell'incidente e determina se aggiornare l'analisi del rischio per il sistema colpito, il gruppo di sistemi o l'intera rete. L'aggiornamento prevede anche la revisione/implementazione delle contromisure interessate dalle nuove minacce.

### *Backup e Recovery*

Le procedure di backup e recovery sono differenti a seconda del tipo di sistema e di importanza dei dati memorizzati. In tutti i casi vengono utilizzate strutture NAS di dischi accessibili direttamente tramite la rete informatica interna.

Il dettaglio della procedura è descritto nel documento riservato ANALISI DEL RISCHIO DELLA RETE MARCEGAGLIA PALINI & BERTOLI.

## Formazione degli Incaricati

La formazione degli incaricati sui temi della sicurezza della rete e dei sistemi che trattano dati personali o strategici di Marcegaglia Palini & Bertoli segue attualmente un iter informale, descritto nei capitoli seguenti.

### *Formazione iniziale*

E' verbale e viene impartita in generale da un Amministratore di sistema, o dal Responsabile sicurezza privacy, per quanto attiene alle regole e norme generali.

Il neoassunto viene indirizzato alla home page intranet del sito Marcegaglia Palini & Bertoli, che attualmente contiene copie elettroniche dei seguenti documenti :

- POLICY DI SICUREZZA;
- PROCEDURA DI SICUREZZA TRATTAMENTI INFORMATICI;
- PROCEDURA DI SICUREZZA TRATTAMENTI CARTACEI;
- PROCEDURA PER IL CORRETTO USO DEL PC;
- PROCEDURA PER IL CORRETTO USO DELLE PASSWORD;
- REGOLAMENTO INTERNO (EMail ed Internet).

nella loro versione più recente.

Una seconda formazione più specifica viene erogata, sempre verbalmente, nella Direzione di destinazione dell'incaricato.

### *Aggiornamenti periodici alla formazione*

Non sono previsti, se non in caso di variazioni delle procedure. Anche in questo caso, vengono erogate verbalmente dai vari responsabili interni di Marcegaglia Palini & Bertoli.

Gli aggiornamenti di documenti e norme sono sempre e comunque segnalati sulla intranet aziendale.

## Controlli sui trattamenti affidati all'esterno

L'obbligo dell'osservanza delle norme, contenute nel Codice e nel GDPR 2016/679 in materia di protezione dei dati personali, viene imposto contrattualmente attraverso specifiche clausole espresse.

Su tutti i trattamenti affidati all'esterno Marcegaglia Palini & Bertoli effettua i controlli prefigurati nelle norme.

## Particolari criteri di sicurezza riservati ai trattamenti di dati sensibili

Le tipologie di dati sensibili non necessitano di separazione dalle tipologie di dati comuni ad esse correlate. Ad es. la base dati del personale (dipendenti/collaboratori), che può contenere dati comuni e dati sensibili (salute), è unica in quanto non esistono gruppi di utenti incaricati al solo trattamento del dato comune, a cui bisognerebbe nascondere il dato sensibile, bensì tutti gli incaricati del trattamento dei dati del personale sono anche incaricati del trattamento della parte sensibile.

## Auditing e controllo del Titolare

Il titolare, attraverso il Responsabile sicurezza privacy, controlla che le policy, le procedure, le regole e le linee guida descritte in questo documento vengano osservate.

Il Responsabile sicurezza privacy relaziona il titolare, su sua richiesta o almeno una volta all'anno, sullo stato degli adempimenti descritti in questo documento.

In occasione di una variazione significativa delle norme o in occasione di una variazione significativa intercorsa alla rete o ai sistemi della Marcegaglia Palini & Bertoli, il Responsabile sicurezza privacy, d'intesa con l'Amministratore di sistema per gli aspetti tecnologici, provvede all'aggiornamento (revisione) di questo documento, compilando opportunamente i frontespizi e dandone notizia al titolare, affinché possa essere inserita, nella relazione accompagnatoria del bilancio, l'asserzione rituale dell'avvenuta redazione/revisione del DPS.

In assenza di variazioni il DPS deve comunque essere revisionato almeno una volta all'anno. In tal caso apporre la dicitura : "Revisione annuale senza variazioni" e far evolvere la numerazione.

## Documenti di riferimento :

1. POLICY DI SICUREZZA
2. PROCEDURA DI SICUREZZA TRATTAMENTI INFORMATICI
3. PROCEDURA DI SICUREZZA TRATTAMENTI CARTACEI
4. PROCEDURA PER IL CORRETTO USO DEL PC
5. PROCEDURA PER IL CORRETTO USO DELLE PASSWORD
6. PROCEDURA PER LA GESTIONE DELLE CASELLE EMAIL
7. PROCEDURA PER LA GESTIONE DELLE UTENZE DI RETE
8. PROCEDURA PER IL RILASCIO DEI PROGRAMMI
9. REGOLAMENTO INTERNO

## Glossario

**addetto** qualsiasi persona fisica che gestisce le rete e i sistemi informatici di Marcegaglia Palini & Bertoli, appartenente alla Direzione Sistemi Informativi;

**amministratore di sistema** una persona fisica che gestisce l'operatività di uno o più addetti;

**autenticazione informatica** l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

**comunicazione** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

**credenziali di autenticazione** i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

**dati sensibili** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

**dato personale** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

**diffusione** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

**incaricati** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

**interessato** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

**parola chiave** componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

**posta elettronica** messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;

**profilo di autorizzazione** l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

**responsabile** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

**responsabile sicurezza privacy** una persona fisica, nominata dal titolare, che adempie in suo nome e conto a tutti gli adempimenti relativi alla funzionalità e sicurezza del sistema informativo Marcegaglia Palini & Bertoli, anche per quanto riguarda gli aspetti del D.Lgs. 196/03 e del Regolamento UE n. 2016/679;

**rete pubblica di comunicazioni** una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

**reti di comunicazione elettronica** i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

**sistema di autorizzazione** l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;

**titolare** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

**trattamento** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

**utente** qualsiasi persona fisica che utilizza la rete e i sistemi informatici di Marcegaglia Palini & Bertoli, non appartenente alla Direzione Sistemi Informativi.