# GDPR su Business

## Indice dei Contenuti

Introduzione e sintesi del GDPR ..... 1
Obblighi per le aziende ..... 2
Le implementazioni in Business ..... 3
Prossimi implementazioni che saranno rese disponibili in seguito ..... 4

## Introduzione e sintesi del GDPR

Il 25 maggio 2018 è entrato in vigore la normativa europea in materia di protezione dei dati personali rappresentata dal Regolamento UE n° 679/2016, comunemente chiamato **GDPR**.

**Riteniamo di fondamentale importanza l'aver partecipato ad uno dei corsi formativi CNA sul tema oppure di aver provveduto in maniera autonoma alla conoscenza degli adempimenti previsti dalla nuova normativa per saper decidere quali azioni intraprendere nell'adeguamento del gestionale Business**

Riportiamo comunque qui solo una estrema sintesi di ciò che il GDPR prevede, per dedicare spazio soltanto a ciò che CNA ha introdotto per rendere **l'uso di Business ed i dati archiviati sul gestionale** adeguabili a questa normativa.

**In sintesi il GDPR prevede quanto segue:**

- Identificazione di specifiche figure e fattispecie coinvolte nella materia:
  - l'interessato, cioè la persona fisica di cui si raccolgono e trattano dati personali di varia natura;
  - il titolare del trattamento dati personali (l'organizzazione che raccoglie e tratta i dati);
  - il responsabile del trattamento: è la persona incaricata dal titolare per il trattamento;
  - l'incaricato trattamento dati (può essere il semplice impiegato che nelle sue mansioni utilizza i dati in oggetto);
  - il Responsabile Protezione Dati (DPO – Data Protection Officer) presente in alcune organizzazioni;
  - l'Autorità di Controllo (in Italia il Garante della Privacy).

- Regole per la raccolta del consenso dell'interessato al trattamento dei suoi dati personali.
- Regole per predisporre l'informativa da fornire all'interessato per le modalità di trattamento.
- Diritti dell'interessato:
  - A conoscere i dati raccolti, ad accedervi, ad averne copia;
  - A chiedere l'oblio, cioè la cancellazione dei suoi dati;
  - A chiedere rettifiche ai dati raccolti;
  - A chiedere limitazioni all'uso dei suoi dati, in attesa di definizione (tipicamente in situazioni di

contenzioso);
- Ottenere la portabilità dei dati (in alcune fattispecie).

 Adempimenti burocratici, come la tenuta di un registro dei trattamenti.

 La predisposizione di misure tecniche (anche e soprattutto informatiche) per garantire la sicurezza dei dati, cioè contro la possibilità di violazione o di uso improprio.

 Alcuni criteri generali per i sistemi informatici al fine di essere in grado di rispettare le norme: la cosiddetta "privacy by default" e "privacy by design".

 L'obbligo di valutare il rischio connesso al trattamento dei dati e l'impatto negativo sugli interessati in caso di violazione.

 L'obbligo di notificare agli interessati eventuali violazione dei dati.

 Linee guida sulle sanzioni da applicare in caso di violazione delle norme (l'applicazione di queste, nel dettaglio, sono lasciate alla normazione da parte dei singoli stati). Si può arrivare anche a sanzioni di importi significativi, per la violazione delle norme sul GDPR.

**È molto importante evidenziare che la normativa non prevede dei requisiti minimi di sicurezza, a differenza di precedenti norme, lasciando al Titolare del Trattamento (quindi ad ogni singola organizzazione) la valutazione e le decisioni sulle procedure e sulle misure di sicurezza (tra cui quelle informatiche) da adottare per tutelare l'azienda dal rischio di perdita o violazione dei dati personali trattati.**
Questo significa che ogni azienda potrebbe esprimere esigenze diverse, in relazione alla natura, oggetto, contesto, finalità e rischi per i diritti e le libertà delle persone fisiche cui i dati trattati si riferiscono.

## Obblighi per le aziende

In sintesi, gli obblighi e i temi che il GDPR introduce per le aziende che tipicamente utilizzano Business possono ricondursi a tre tipologie:

 **Obblighi organizzativi e burocratici**
La CNA offre questo servizio con consulenti specializzati sulla materia (privacy@cnafc.it).

 **Misure di sicurezza informatica**
Misure che non riguardano specificatamente la parte applicativa di Business, bensì l'infrastruttura informatica su cui Business viene utilizzato; si tratta di temi, misure e configurazioni di tipo sistemistico, legati all'uso dei sistemi operativi, dei database, delle reti.
Anche per questo aspetto la CNA offre questo servizio con consulenti specializzati sulla materia (assistenza@cnafc.it)

 **Funzionalità del sistema gestionale Business** e di ogni sistema informatico presente in azienda.
Funzionalità che consentono agli utenti di gestire al meglio i dati personali in linea con i principi generali stabiliti dal GDPR. Per esempio: un adeguato sistema di gestione delle password e di identificazione degli utilizzatori (incaricati) del sistema informativo gestionale.

L'impegno di CNA su quest'area riguarda l'introduzione in Business di una serie di nuove funzioni per rispondere alle norme generali di protezione dei dati.

**Solo questo è l'oggetto del presente documento** ed è descritto nelle pagine che seguono.

## Le implementazioni in Business

**La normativa non impone obblighi alle organizzazioni di adeguare/cambiare i sistemi informatici preesistenti, è però richiesto al Titolare del Trattamento l'obbligo di verificare e integrare le misure adeguate al momento dell'acquisizione di un nuovo prodotto/servizio, per rispettare il GDPR, nonché preoccuparsi di adottare le misure necessarie a supporto dei sistemi esistenti.**

E' necessario quindi che il **Titolare del Trattamento** ci fornisca indicazioni su ciò che ritiene di voler attivare circa le nuove funzionalità offerte da Business, tenendo presente che ognuna di queste ha lo scopo di coprire una delle richieste del GDPR ma che potrebbe influire sull'attuale modus operandi e/o essere invalidata da cattivi comportamenti al di fuori del gestionale

Ragione Sociale azienda:

_____

Numero Posti di lavoro: ☐ data compilazione: ☐

Titolare del Trattamento ☐

Vi invitiamo a completare queste informazioni indicando Si ☐ o No ☐ sulle funzionalità che voler far attivare dai nostri tecnici

Si ☐ No ☐ **Potenziamento password :** Potenziamento di tutto il sistema della gestione dell'autentificazione login/password (per esempio: gestione password complesse, password a scadenza, con obbligo di cambio periodico, funzioni di reset password, crittografia delle password non decriptabile (con algoritmi standard riconosciuti)
**Scopo**: rispetta i requisiti imposti dal GDPR circa le password di accesso a Business
**Difetti**: Impone digitazione password all'accesso e può complicare l'attivazione di procedure automatiche pianificate (estrazione dati datawarehouse ecc…), impone cambio password in 180 giorni

Si ☐ No ☐ **Creazione di singoli utenti**: se si usano utenti comuni (esempio "Admin") suggeriamo di creare utenti specifici, con nome, cognome, email e password complesse, eventuale copia delle configurazioni di altri utenti con cui si è sempre lavorato
**Scopo**: Permette una profilazione ottimale delle maschere con disposizione controlli, dimensioni form e 'recenti' specifici per utente, rende gestibile il cambio password con la segretezza della stessa.
N.B.: preparare un elenco con NOME UTENTE, NOME, COGNOME ed EMAIL per agevolare il tecnico

Si ☐ No ☐ **Abilitazione LOG completi** per accesso ai programmi ed inserimenti oltre che modifiche e cancellazione di informazioni
**Scopo**: Permette il log di tutte le attività compreso accesso ai programmi e le operazioni (tranne le interrogazioni e stampe) su Business tracciato per utente
**Difetti**: nel caso il database cresca di dimensioni sarà necessario cancellare i log di un periodo molto vecchio

Si ☐ No ☐ **Criptazione di tutto il traffico dai client verso il database SQL di Business**
**Scopo**: una eventuale intercettazione del traffico di Business sulla rete interna da parte di un malintenzionato collegato alla rete, non ne permetterebbe la lettura

Si ☐ No ☐ **Restrizione dell'accesso al database creando utenti specifici su SQL Server con accessi mirati ai database da usare e funzionalità** corrispondenti agli utenti di Windows senza permettere accesso ad utenti solo di SQL (autenticazione trusted di MS-SQL)
Scopo: Rende molto più sicuro l'accesso ai dati, non basandolo più su di un utente AMMINISTRATORE uguale per tutti di cui può essere facile trovare la password, ma rende questo accesso condizionato all'utente con cui si è entrato in Windows
**Difetti**: Eventuali nuove postazioni di Windows, che dovranno accedere a Business, necessitano di una configurazione utenti di SQL corrispondente
Eventuali altri programmi che leggono o scrivono sui database dovranno farlo usando utenti di Windows specifici e non un accesso generico

Si No **Criptazione delle password accesso ai database di procedura ed aziendali**

Questa funzionalità potrebbe essere intesa come alternativa al punto precedente
**Scopo**: Nasconde i percorsi di accesso ai dati di SQL, oltre che la password dell'utente con cui tentarne l'accesso, in nessun modo è possibile capire dove risiedono i database
**Difetti**: Se non fa accesso a Business i dati non sono rintracciabili sulla rete

Si No **Cifratura delle cartelle dei database di Business**

**Scopo**: I file di dati di Business, se copiati in chiaro, sono decifrabili con appositi strumenti, attivando la cifratura della cartella su cui sono archiviati, i dati sono crittografati e la copia di questi file su altri computer non è leggibile in nessun modo.
**Difetti**: il rallentamento dovuto alla cifratura è di circa dall' 1% al 3%

Si No **Cifratura delle cartelle e dei supporti di backup o adozione di backup in cloud**

**Scopo**: il backup fatto da Business se posizionato su di cartella non cifrata, sarebbe leggibile da chi ne entra in possesso anche se i dati originali sono su di una cartella cifrata, in questo modo l'intero spazio di backup ha lo stesso livello di sicurezza (rispetto alla lettura non autorizzata)
**Difetti**: Nel caso di supporti rimovibili cifrati il backup potrebbe essere ripristinabile solo sul PC da cui è avvenuta la criptazione.
Il backup sul cloud invece permette la lettura ed il ripristino (dietro verifica delle credenziali) su qualunque altra postazione vogliate riportare i dati

**Il nostro consiglio è di adottare uno strumento di backup che effettui un primo salvataggio cifrato in locale ma ANCHE una copia sul cloud in modalità cifrata, così da avere la copia sempre disponibile ma al sicuro da accessi non autorizzati.**

## Prossimi implementazioni che saranno rese disponibili in seguito

**Funzione di anonimizzazione** : Realizzazione di una funzione di anonimizzazione dei dati (per soddisfare il diritto all'oblio), mascherando i dati personali con stringhe di "*" (asterischi) o altro carattere speciale (operazione non reversibile); tale funzione sarà pilotata dall'utente su singoli cli/for o su liste

**Altri campi e logiche legate alla privacy :** Gestione di altri campi come: data scadenza autorizzazione trattamento dati, data prestazione consenso, data revoca consenso, modalità di acquisizione del consenso

**Produzione lettere raccolta consenso e informative :** Realizzazione di un programma che permetta di produrre lettere di richiesta autorizzazione al trattamento dei dati (raccolta consenso, informativa), partendo da clienti/fornitori/liste selezionate, con possibilità di invio. Testo della lettera modificabile (modello di word).
Nel frattempo potranno essere utilizzate le funzioni già esistenti di stampa su word da lista selezionata, con apposito modello di word.

**Export dati personali :** Funzione per esportare i dati personali di un soggetto interessato, in flat-file, a chi ne fa richiesta

**Protezione oggetti OLE e altri files :** Implementazione per far sì che gli oggetti OLE, gli allegati alle mail, i file in cartella ASC e in cartella Office, possano risiedere opzionalmente in un contenitore (cartella/e) con accesso riservato a specifici utenti di Business ma senza poterne avere accesso da windows
Altri campi e logiche legate alla privacy : Gestione di altri campi come: data scadenza autorizzazione trattamento dati, data prestazione consenso, data revoca consenso, modalità di acquisizione del consenso …

CNA SERVIZI FORLI' CESENA
AREA ICT

Commerciale
Tel. 0543 770350

Assistenza
Tel. 0543 770351
assistenza@cnafc.it