Privacy & Regolamento 679
Consulenza & Formazione per Aziende e Professionisti

GDPR
GENERAL DATA PRIVACY REGULATION
REGOLAMENTO 679:2016

SEMPLICE GUIDA ED INFOGRAFICA
PRIVACY PER MICROIMPRESE

Sommario

1- PREMESSA

Con questa semplice Guida ti voglio offrire un panorama delle principali problematiche che le MICRO IMPRESE dovranno tenere presenti in vista della piena applicazione del regolamento, prevista il **25 maggio 2018**.

Per **MICRO IMPRESA** intendo una piccola società o ditta individuale sotto i 10 dipendenti e sotto i 2 Milioni di € di fatturato.
Lo scopo è di rendere più agevole il passaggio al nuovo regolamento con una serie di esempi che potranno guidarti nell'applicazione pratica di ciò che ci sarà da fare, evitando così che tu possa incappare in errori e pesanti sanzioni.

Ti saranno fornite alcune raccomandazioni specifiche su cosa dovrai fare sin da ora perché ci sono disposizioni molto precise del regolamento che non lasciano spazi a interpretazioni.

Ti indicherò inoltre, e per il tuo ambito specifico, alcune delle principali novità introdotte dal Nuovo Regolamento 679 rispetto alle quali cercherò di suggerirti possibili approcci in modo da essere preparato all'appuntamento del 25 maggio 2018 con le idee più chiare.
Buona lettura.

2- Organizzazione

Come prima cosa dovrai definire una serie di figure chiave nella tua organizzazione anche se è piccola.
Nello specifico di dico quali tali figure e cosa dovrai fare:

TITOLARE DEL TRATTAMENTO DEI DATI

Nel caso delle MICRO IMPRESE il Titolare del Trattamento è l'amministratore della società, colui che di fatto ha la responsabilità legale dell'azienda. Quindi è molto semplice, non ci possono essere fraintendimenti.

RESPONSABILE DEL TRATTAMENTO DEI DATI

A meno che tu non abbia una organizzazione complessa non è necessario nominare un ulteriore Responsabile per il trattamento dei dati. Questo può essere sostituito eventualmente con un consulente esterno esperto in materia con il quale stabilire incontri periodici almeno semestrali per verificare che tutte le cose siano fatte nel modo corretto.

INCARICATI DEL TRATTAMENTO DEI DATI

Gli incaricati sono tutte quelle persone che operativamente trattano i dati nella tua azienda, sia dipendenti interni ma anche i consulenti esterni.
Ti faccio un esempio:

- Amministrazione: dati di clienti e fornitori
- Risorse Umane: dati dei dipendenti
- Resp. Commerciale: dati dei clienti
- Consulente del lavoro: dati dei dipendenti
- Commercialista: dati di clienti e fornitori
- Consulente informatico: tutti i dati in azienda

A tutti gli incaricati dovrai far firmare specifiche lettere di consenso che dopo ti spiegherò meglio.

3- Sistemi Informatici

Rientrano nella tua organizzazione anche i sistemi informatici che utilizzi per la tua attività ed i vari collegamenti esterni.

Quali sono i passi che dovrai fare? Seguimi e te li dirò.

- Devi procedere con un elenco dei vari sistemi informatici che utilizzi (p.es. pacchetto office, eventuali applicativi specifici come programma di fatturazione, CRM, ecc.) e rendere disponibili le licenze;
- Elencare i vari utenti che utilizzano i programmi infirmatici e quali modalità di accesso hanno;
- Elencare quali sistemi ANTIVIRUS o FIREWALL stai utilizzando e che tipo di protezione hai attivato;
- Fare un elenco delle varie e-mail aziendali, chi ne possiede l'accesso e come sono stabilite le credenziali di autenticazione (PASSWORD)
- Definire il tuo sistema di salvataggio dei dati informatici, frequenza e modalità di salvataggio;
- Se utilizzi sistemi in Cloud avere chiaro come vengono archiviati i tuoi dati e su quali server, se sono residenti in territori Italiani, Europei o fuori dai confini Europei;
- Ti suggerisco inoltre di affidarti ad un consulente informatico che ti possa aiutare a gestire tali attività.

4- Tipologia dei dati trattati [Finalità e Scopi]

Un punto chiave della nuova privacy sarà stabilire con esattezza le Finalità ovvero gli Scopi per cui hai necessità di trattare e gestire alcuni dati nella tua azienda.
Per fare questo un semplice passo è quello di predisporre una tabella (come quella che ti indico nel seguito) nella quale inserire gli ambiti, le tipologie di

dati e le finalità che possono essere presenti nelle diverse tue attività aziendali:

AMBITO	TIPO DI DATO	FINALITA' / SCOPI
Clienti e fornitori	Dati societari Dati bancari Nomi e cognomi persone	Gestione Amministrativa / Contabilità
Gestione del personale	Nomi e Cognomi lavoratori Cartella sanitaria Dati Bancari	Gestione Contabile / Amministrativa
Bilancio (Commercialista)	Dati di clienti e fornitori Dati giudiziari (Ag. Entrate / FINANZA / Ecc.)	Gestione Contabile / Amministrativa
Consulente Informatico / provider	Tutti i dati societari gestiti a livello informatico Gestione PW	Archivio e back up dati

Ovviamente si tratta solo di un esempio che tu dovrai completare con i tuoi specifici dati e le relative finalità

5- Valutazione dei rischi

Dopo aver fatto la tua mappatura delle varie tipologie di dati e le finalità dovrai stabilire una modalità relativa la valutazione dei rischi.

Ovvero indicare in termini numerici qual è il livello di probabilità e quindi il RISCHIO che un dato possa essere violato.
Un esempio che tu può aiutare è quello che ti propongo nel seguito in cui viene appunto effettuata una valutazione del grado di rischio che incombe sulla gestione e trattamento dei dati siano essi cartacei che elettronici.

I rischi sono identificati in funzione:

- Del tipo di dato
- Di come viene effettuato il trattamento
- Di chi effettua il trattamento
- Di quale impatto / conseguenze il rischio può avere

Al fine di poter oggettivare la Valutazione del Rischio, le sue componenti vengono suddivise nelle seguenti macro tipologie:

1. **RISCHIO DI AREA**: che dipende dal luogo dove gli strumenti sono ubicati.

Tale rischio è legato sostanzialmente:

- Al verificarsi di eventi distruttivi (incendi, allagamenti, corti circuiti);

- Alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici);

2. **RISCHIO LEGATO AL COMPORTAMENTO DEGLI OPERATORI**:

- Furto di credenziali di autenticazione;
- Carenza di consapevolezza, disattenzione o incuria;
- Comportamenti sleali;
- Errore umano.

3. **RISCHIO LEGATO AGLI STRUMENTI UTILIZZATI**:

- Azione di virus informatici;
- Spamming o altre tecniche di sabotaggio;
- Malfunzionamento o degrado degli strumenti;
- Accessi esterni non autorizzati;
- Intercettazione di informazioni in rete.

Vedi nella pagina seguente un esempio di matrice di valutazione rischi.

RISCHIO DI AREA Tab. 1

EVENTO	Impatto sulla sicurezza dei dati		Misure di prevenzione attuate	Misure di prevenzione Attuare
	Descrizione	Gravità evento		
1.1. Accessi da parte di terzi non autorizzati	Nel normale orario di lavoro si accede in azienda facendosi riconoscere al videocitofono. Le persone esterne sono accolte all'ingresso e non hanno possibilità di accedere autonomamente ai documenti cartacei e/o informatici.	1	Il personale esterno è sempre accompagnato da personale aziendale. Non è possibile accesso autonomo da parte di terzi.	Al momento nessuna.
1.2 Asportazione e furto di strumenti informatici / cartacei contenenti dati.	L'azienda dotata di impianto di allarme perimetrale e volumetrico. La ditta Cittadini dell'ordine Srl effettua controllo esterno dei locali ed inoltre contatta Atempo Spa in caso di intrusione o di allarme.	2	Regole di comportamento e controllo giornaliero	Al momento nessuna.
1.3 Eventi distruttivi naturali, dolosi o accidentali dovuti ad incuria.	Per quanto concerne il rischio incendio sono presenti nei locali adeguati sistemi antincendio così come previsto dal D.Lgs. 81/08 e 106/09	1	Verifica semestrale degli estintori da parte di ditta specializzata.	Al momento nessuna.
1.4 Guasti o malfunzionamenti ai sistemi supplementari (impianto elettrico, climatizzazione, ecc.)	L'impianto elettrico è stato realizzato in conformità alla L. 46/90. Eventuale innesco di incendio viene gestito come sopra riportato.	1	Verifica semestrale degli estintori da parte di ditta specializzata. Verifica biennale della messa a terra dell'impianto elettrico.	Al momento nessuna.
Valutazione media rischio di AREA	**1,25**			

Sulla base del risultato della valutazione dei rischi dovrai stabilire l'eventuale tuo piano di azioni o di mantenimento della situazione conforme.

6- Lettere di consenso e di riservatezza

Occorre prima fare un doveroso distinguo tra cosa significa **CONSENSO** e cosa significa **RISERVATEZZA**.

Il **consenso** sarà necessario verso tutti coloro i quali tratti dei dati specifici. Quindi di nuovo parliamo di:

- Dipendenti
- Consulenti

- Fornitori
- Clienti

Dovrai a questo punto preparare delle specifiche lettere di consenso che dovrai inviare a tutti i soggetti di cui sopra spiegando loro che tipologie di dati trattati, le finalità e gli scopi. Dovrai farle firmare e fartele restituire, e soprattutto fare attenzione ad archiviarle e tenerle sempre e costantemente disponibili. Dovrai ripetere questa operazione ogniqualvolta aggiungerai un dipendente, cambierai un fornitore o aggiungerai un cliente.

La **RISERVATEZZA** invece si riferisce più ad una tua tutela, ovvero al fatto di garantire che i TUOI dati aziendali, le TUE INFORMAZIONI, il TUOI KNOW-HOW non vengano trafugati dai tuoi dipendenti o collaboratori, sia durante le attività lavorative che eventualmente a fine rapporto.
Devi predisporre quindi una specifica lettera da far firmare ad ogni dipendente e collaboratore con la quale vendono definire in modo chiaro le regole di riservatezza aziendale.

7- Diritto all'Oblio

Questo è un requisito nuovo nel panorama Privacy.

Si tratta del fatto che nel momento che il rapporto di lavoro viene a cessare, per esempio un dipendente si licenzia, o viene cambiato un fornitore, oppure un cliente cessa di essere cliente, tutti i dati sia in forma cartacea che informatica dovranno essere eliminati.

Tu dovrai quindi comunicare a questi soggetti le modalità di eliminazione e distruzione dei propri dati al fine di rispettare appunto questo diritto all'oblio.

8- TUTELA DEI MINORI di età inferiore ai 16 Anni

Se la tua azienda accoglie personale minore con età inferiore ai 16 anni, dovrà iniziare a pensare a mettere in atto i sistemi per verificare l'età delle persone e per raccogliere il consenso dei genitori o dei tutori per l'elaborazione dei dati personali.

Le attività più comuni dove questo si rende necessario sono: SCUOLE, PALESTRE, ASSOCIAZIONI SPORTIVE, ATTIVITA' SOCIAL ecc.

Infatti per la prima volta, il NUOVO REGOLAMENTO PRIVACY introdurrà una **protezione speciale per i dati personali dei minori** in particolare nel contesto dei servizi commerciali in rete come i social network.

I minori infatti meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali.
In breve, se un'azienda raccoglie informazioni sui minori allora avrà bisogno del consenso di un genitore o di un tutore per elaborare i loro dati personali in modo lecito.

Questo potrebbe avere implicazioni significative se l'azienda fornisce servizi ai bambini e raccoglie i loro dati personali. Il consenso deve essere sempre verificabile e quando vengono raccolti i dati sui minori è necessario definire una specifica informativa per la privacy in un linguaggio che sia comprensibile ai minori.

9- Consapevolezza & Formazione

Per conoscere le regole del nuovo regolamento privacy e quindi esserne pienamente consapevole è necessario che tu ed i tuoi dipendenti riceviate una Formazione adeguata per comprendere appieno la portata di questa nuova legge.
Non c'è nulla di difficile ma certamente è necessario capire i punti chiave anche solo per evitare il rischio di incorrere in **PESANTI SANZIONI**

Ti proponiamo quindi specifiche sessioni di formazione che troverai nel nostro sito web www.regolamento679.com sia per te Titolare di Impresa che per i tuoi lavoratori.

10- PROPOSTA Privacy Facile per MICRO IMPRESE

Ma sappi che tu in qualità di MICRO IMPRESA potrai aderire al progetto

PRIVACY FACILE!

Un'offerta **"TUTTO COMPRESO"** per fare in modo che tu abbia tutti i documenti e sia "in regola" velocemente e senza troppi sacrifici.
Per te la questione Privacy non è mai stata così FACILE!

COSA TI FORNIREMO CON **PRIVACY FACILE**:

- *Elaborazione del DDMS Documento Descrittivo delle Misure di Sicurezza*
- *Mappatura e Valutazione dei rischi in materia di Privacy e trattamento dei dati*
- *Lettere di consenso dipendenti, clienti e fornitori*
- *Nomine del Titolare dei Responsabili e degli Incaricati*
- *Predisposizione lettere di Riservatezza dei dati aziendali*
- *Formazione di base sui requisiti del nuovo Regolamento 679*
- *Iscrizione gratuita al nostro Magazine: La gazzetta della Privacy*

Non rischiare pesanti sanzioni soltanto per evitare di affrontare adesso questo peso.
Con noi di Privacy e Regolamento 679 puoi evitare di pensarci ancora!


Periodico – N°1 COPIA OMAGGIO
REGOLAMENTO 679
La Gazzetta Della Privacy
La tua informazione libera nel mondo della gestione e trattamento dei dati
PERICOLOSE SANZIONI
FINO AL 2 % DEL FATTURATO MONDIALE DELLA SOCIETA'
PRIVACY E SECURITY dei Sistemi Informatici Flow Chart
Trasforma le tue attività in PROCESSI AZIENDALI
PRIVACY FACILE per abbattere la BUROCRAZIA

11- IL TUO INCUBO PEGGIORE ??

*Svegliarti un giorno, quel giorno, il **24 Maggio 2018** e scoprire che la tua AZIENDA **non è in regola** con gli adempimenti burocratici previsti dal NUOVO REGOLAMENTO 679:2016 sulla PRIVACY*

*Abbiamo ancora qualche mese per adeguarci, infatti le sanzioni vertiginose (20 milioni di € o il 4% del fatturato mondiale) portate dal nuovo Regolamento 679/2016, oggi sono fortunatamente in standby e rimarranno tali **fino al 24 Maggio 2018**.*

Dopo di che TRASGRESSORI: OCCHIO AL VOSTRO PORTAFOGLI!

SAPPIATE CHE DAL 1° GENNAIO 2018 MANCHERANNO SOLO

144 GIORNI

CHI SONO

STEFANO SCANAVINO

Consulente esperto in ambito privacy sin dalla Legge 675/96.

Ad oggi si occupa di Consulenza in materia di privacy compliance e protezione dei dati, implementazione e mantenimento Sistema Privacy di Gestione della Sicurezza dei Dati (SGSD), audit di verifica e risk assessment, Rapporti di Audit, Data Protection Impact Assessment, Piano Azioni Correttive, ecc.), gestione di Modelli Organizzativi specifici (Videosorveglianza, Controllo Accesi, Policy IT, Sistemi di Geo localizzazione Satellitare, ecc.), Sistemi di Gestione Integrati: Privacy & Qualità.

Nelle aziende cliente assume incarico di D.P.O [Data Protection Officer]

European Privacy Auditor secondo Norma ISDP©10003:2015

COME FACCIO A SAPERNE DI PIU'

Puoi visitare il nostro sito www.regolamento679.com
o chiamando il nostro numero

Attivo 24/24 e 7/7 +393664515806

Direttamente da sito potrai scaricare

RISORSE GRATUITE

Puoi collegarti alla nostra pagina FACEBOOK
REGOLAMENTO679

Privacy & Regolamento 679
Consulenza & Formazione per Aziende e Professionisti