Organizzazione

AZIENDA s.p.a.

Via Mazzini, n. 56 – 20100 Milano (MI)

Tel. 0287654321 - Fax. 0287654321

Web : www.nomeazienda.it

E-Mail : info@nomeazienda.it

Documenti privacy per adempiere al Regolamento Europeo 679/2016 GDPR

Master	√
Copia controllata	√
Copia non controllata	×
Numero della copia	02

Emissione	Data		Firma	
Approvazione	Data		Firma	

Stato delle revisioni

Versione	Data	Descrizione	Autore
00	*04/12/2018*	Prima emissione	Mario Rossi
01	*10/01/2019*	Modifiche alla sezione 0.3	Elisa Autieri
03	***04/04/2019***	**Modifiche alla sezione 1.2**	Carlo Campagna

0 Premessa

Questa Check List è stata progettata ed elaborata quale supporto all'adeguamento ed all'implementazione di un sistema GDPR conforme al REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 Aprile 2016 relativo alla protezione dei dati delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Trattasi della prima Check List in Italia consultabile liberamente e gratuitamente per la verifica di conformità ai vari articoli del GDPR.

Questa Check List consente di monitorare periodicamente lo stato di adeguamento del sistema GDPR, nel caso in cui l'organizzazione stia gestendo questo aspetto, o di controllare l'implementazione di un sistema GDPR in riferimento al REGOLAMENTO (UE) 2016/679

Come già emerso in vari ambiti e convegni, le novità e le modifiche apportate dal REGOLAMENTO (UE) 2016/679 sono notevoli ed incidono in modo sostanziale sui comportamenti nelle Organizzazioni in merito al trattamento dei dati personali, nonché alla libera circolazione di tali dati

La eventuale sottovalutazione di alcuni articoli specifici, oltre a non rendere il sistema GDPR aderente al REGOLAMENTO (UE) 2016/679 rischia di evidenziare maggiormente alcuni aspetti di errata gestione aziendale che possono andare oltre una semplice non conformità.

Per questo motivo è necessario iniziare ad effettuare tutte le valutazioni di impatto legate al recepimento del nuovo Regolamento, onde evitare la gestione frettolosa di alcuni aspetti gestionali ed operativi.

In tale ambito, la Check List elaborata può essere uno strumento importante, utilizzato unitamente ad altri strumenti tecnici, anche per la corretta gestione dell'attività di audit allo scopo di sorvegliare l'adempimento dei requisiti del GDPR e l'applicazione delle misure tecniche ed organizzative all'interno dell'Organizzazione e all'esterno di questa nell'ipotesi di trattamenti affidati a responsabili esterni.

Check List – Verifica conformità ed adeguamento RE 679/2016 | **CHECK LIST-01**

1 Check-list di conformità – GDPR Privacy 2018

Art. GDPR	Documenti da produrre	Azioni	C	NC	Descrizione non conformità
30	Registro dei trattamenti	È stato compilato il registro dei trattamenti?	☐	☐	
		Il registro dei trattamenti è aggiornato?	☐	☐	
32	Sicurezza del trattamento (Valutazione rischi) Misure tecniche e organizzative	È stato compilato il documento di valutazione dei rischi?	☐	☐	
		È tenuto aggiornato il documento di valutazione dei rischi?	☐	☐	
		Risultano applicate le misure tecniche inserite nel documento?	☐	☐	
		Risultano applicate le misure organizzative inserite nel documento	☐	☐	
		Si effettuano controlli sulle misure tecniche eseguite?	☐	☐	
		Si effettuano controlli sulle misure organizzative eseguite?	☐	☐	
35	Documento di valutazione di impatto privacy	È stato verificato l'obbligo della valutazione di impatto?	☐	☐	
		È stata accertata la necessità di nominare il DPO?	☐	☐	
		Se obbligatorio, è stato compilato il documento di valutazione di impatto?	☐	☐	
		Se obbligatorio, è tenuto aggiornato il documento di valutazione di impatto?	☐	☐	
36	Consultazione preventiva	È stato verificato l'obbligo della consultazione preventiva?	☐	☐	
		Se sì, è stata inoltrata la richiesta di parere?	☐	☐	
		Se sì, sono state eseguite le prescrizioni segnalate dal Garante?	☐	☐	
		Viene effettuato il controllo sulle prescrizioni eseguite?	☐	☐	

Check List – Verifica conformità ed adeguamento RE 679/2016

CHECK LIST-01

33,34	Procedura data breach	È stato individuato un ufficio responsabile?	☐	☐	
		È stato preparato un protocollo azioni (anche per i responsabili esterni)?	☐	☐	
		Sono eseguite le misure tecniche e organizzative inserite nel protocollo?	☐	☐	
		Viene verificata la sussistenza cause di esonero?	☐	☐	
		Si è preparati per l'invio delle notificazioni (iniziali ed integrative) al Garante?	☐	☐	
		Si è preparati per l'esecuzione delle prescrizioni del Garante?	☐	☐	
		È stato realizzato il modulo di invio di comunicazione agli interessati?	☐	☐	
		È presente il registro della violazione dei dati?	☐	☐	
26	Accordo con contitolari	Esiste il documento che stabilisce un accordo di contitolarità?	☐	☐	
		Al suo interno sono stabilite le misure organizzative e tecniche previste dall'accordo	☐	☐	
		È stato previsto un punto di contatto unico nei confronti degli interessati?	☐	☐	
28	Contratto di responsabile esterno	È stata realizzata la mappa dell'esternalizzazione dei trattamenti?	☐	☐	
		Sono compilati i contratti con i responsabili esterni?	☐	☐	
		Sono eseguite le misure normative, tecniche e organizzative previste dal contratto?	☐	☐	
		Sono programmati ed eseguiti i controlli del responsabile esterno?	☐	☐	
		È stato sottoscritto il patto di riservatezza con i dipendenti del responsabile esterno?	☐	☐	
		È stato verificato l'allineamento dei contratti in essere con il modello legale?	☐	☐	

Check List – Verifica conformità ed adeguamento RE 679/2016

CHECK LIST-01

		Se l'allineamento non è perfetto è stata effettuata la stesura di modifiche e sottoscrizione delle clausole aggiuntive/sostitutive?	☐	☐	
28	Contratto con sub responsabili	È stata preparata una mappatura della sub esternalizzazione dei trattamenti?	☐	☐	
		Se sì, è stata effettuata la stesura di apposite clausole nei contratti con i responsabili esterni?	☐	☐	
		Se sì, vengono pianificate ed eseguite le procedure selettive previste nelle clausole contrattuali?	☐	☐	
		Se sì, vengono pianificati ed eseguiti controlli per il tramite del responsabile esterno?	☐	☐	
5	Atto di nomina e disciplinare	È stata effettuata la mappatura delle nomine esistenti e viene verificato il mantenimento di centri apicali interni?	☐	☐	
29	Nomina dipendenti e collaboratori	È stata effettuata la mappatura delle posizioni dei soggetti interni che trattano i dati?	☐	☐	
		Si effettuano verifiche per la profilazione del personale interno?	☐	☐	
39	Corsi per gli autorizzati	Vengono svolti i corsi base per autorizzati al trattamento?	☐	☐	
		Vengono svolti corsi per livelli apicali?	☐	☐	
		Se necessario, vengono preparati corsi per il DPO interno?	☐	☐	
12,13,14	Informativa	È stata verificata la necessità del consenso?	☐	☐	
		Sono state preparate le informative?	☐	☐	
		Sono state apportate le icone alle informative?	☐	☐	
		È stato istituito un ufficio per risposte alle richieste degli interessati?	☐	☐	
		È stato redatto un protocollo per le attività dell'ufficio "trasparenza"?	☐	☐	
6,7,8,9	Raccolta consensi	Per la raccolta del consenso sono state	☐	☐	

Check List – Verifica conformità ed adeguamento RE 679/2016

CHECK LIST-01

		predisposte formule in linea con il GDPR?			
		In caso di minori di età, ai fini della raccolta del consenso, sono state previste cautele particolari?	☐	☐	
		Sono stati preparati procedure e moduli per la gestione delle revoche del consenso?	☐	☐	
6,9	Condizioni di liceità diverse dal consenso	Sono state verificate condizioni di liceità diverse dal consenso?	☐	☐	
		È stata verificata la presenza delle cautele in linea con il GDPR?	☐	☐	
6	Legittimo interesse (trattamenti con uso di nuove tecnologie e strumenti automatizzati)	Sono stati verificati i presupposti del legittimo interesse?	☐	☐	
		È stata inviata l'informativa al Garante (legge 205/2017, art 1, comma 1022)?	☐		
		Se sì, viene dato riscontro a richieste istruttorie del Garante (legge 205/2017, art 1, comma 1023)?	☐		
		Se sì, vengono eseguite le prescrizioni del Garante?	☐		
37,38,39	Nomina RPD/DPO policy interna	È stata effettuata la verifica obbligo/opportunità della nomina del DPO?	☐		
		Se sì, la scelta del DPO ha considerato entrambe le ipotesi tra dipendente oppure professionista/organizzazione esterna?	☐		
		Se sì, è stato redatto e sottoscritto il contratto?	☐	☐	
		Se sì, è' stata effettuata la comunicazione al Garante dell'avvenuta nomina del DPO?	☐	☐	
		Se sì, vengono eseguite le misure previste nel contratto?	☐	☐	
		Se sì, è stato Istituito un ufficio del DPO?	☐	☐	
		Se sì, è stato istituito un punto di contatto del DPO con gli interessati?	☐	☐	
44-50	Condizione di liceità	Vengono verificate e rispettate le	☐	☐	

Check List – Verifica conformità ed adeguamento RE 679/2016

CHECK LIST-01

		condizioni di liceità (ad es. BCR, Codici di condotta, Certificazione, Clausole contrattuali, Consenso/Legittimo interesse…)?			
		I documenti ed i contratti sono sottoscritti in base alla condizione di liceità applicabile?	☐	☐	
		Vengono eseguite le cautele imposte dal Garante o dal contratto o dalle altre condizioni di liceità?	☐	☐	
		Vengono verificati i trasferimenti dei dati al di fuori dell'UE a cavallo del 25/05/2018 e l'eventuale allineamento al GDPR	☐	☐	
42,43	Certificazione	È stata valutata l'ipotesi della certificazione?	☐	☐	
		Esecuzione misure di mantenimento	☐	☐	
40,41	Codice di condotta	Adesione a codice di condotta	☐	☐	

Luogo e data

Firma titolare trattamento