VALUTAZIONE DI CONFORMITÀ CON IL GDPR

effizient COMPANY SOLUTIONS

Partner 24ORE

PREMESSA

Il presente documento è stato predisposto prendendo spunto dal "listado de cumplimiento normativo" elaborato dall'AEPD (Autorità di controllo spagnola) che, nella sua versione originaria, è reperibile al seguente indirizzo: https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf.

Alcune verifiche sono state adattate alle specificità del quadro normativo "privacy" vigente in Italia alla data di redazione del documento.

Non si tratta di una traduzione ufficiale né perfettamente aderente alla versione elaborata dall'AEPD; l'elenco di controlli sotto proposti è meramente esemplificativo ed è stato pensato come strumento di supporto alle attività di verifica svolte dal Titolare e/o dal Responsabile del trattamento.

La "check-list" è prettamente rivolta a quanto previsto dal Regolamento generale per la protezione dei dati personali 2016/679 (GDPR): potrebbero risultare pertanto esclusi alcuni specifici provvedimenti, linee guida, indicazioni operative formulati sia in ambito italiano che europeo.

La compilazione del presente documento non esonera dalle responsabilità previste dalla vigente normativa e permane sul Titolare e/o sul Responsabile del trattamento la valutazione di adeguatezza del suo contenuto rispetto al trattamento ed alla realtà che si analizzano.

effizient COMPANY SOLUTIONS Partner 24ORE

VALUTAZIONI DI CONFORMITÀ CON IL GDPR	SI / NO

PRINCIPI DI TRATTAMENTO

I dati personali sono raccolti per scopi specifici?	
I dati personali sono raccolti per scopi espliciti?	
I dati personali sono raccolti per scopi legittimi?	
Sono ulteriormente trattati in modo incompatibile con altri scopi?	
I dati personali sono mantenuti in maniera accurata?	
I dati personali vengono aggiornati?	
I dati personali inesatti vengono rettificati in base alla finalità del trattamento?	
I dati personali che sono inesatti rispetto alla finalità del trattamento vengono cancellati?	
I dati personali sono conservati più a lungo di quanto necessario in base alla finalità del trattamento? Se sì:	
Vengono elaborati per scopi archivistici per pubblico interesse?	
Vengono trattati per scopi di ricerca scientifica?	
Sono trattati per scopi storici?	
I dati personali sono trattati per scopi statistici	
Sono state implementate misure di sicurezza atte a proteggere l'integrità e la riservatezza dei dati?	
Sono state implementate misure di sicurezza volte a prevenire il trattamento non autorizzato o illecito di dati personali?	
Sono state implementate misure di sicurezza adeguate a prevenire perdite accidentali, distruzione o danneggiamenti accidentali di dati personali?	
Viene mantenuta la tracciabilità delle finalità del trattamento?	

LICEITA' DEL TRATTAMENTO

Qualora il trattamento si basi sul consenso, questo viene conferito per ogni finalità?	
Il trattamento è necessario per esecuzione di un contratto o per la fase precontrattuale?	
Il trattamento viene svolto in virtù di un obbligo legale?	
Il trattamento è necessario a proteggere un interesse vitale dell'interessato?	
Il trattamento è necessario per lo svolgimento di un compito di interesse pubblico?	
Il trattamento si basa su un interesse legittimo? Se sì:	
È dimostrabile il bilanciamento di interessi compiuto?	
Per fornire un servizio vengono richiesti solo dati necessari?	
Per eseguire un contratto, vengono richiesti solo i dati necessari?	

CONDIZIONI PER IL CONSENSO

Il consenso conferito dall'interessato è dimostrabile?	
Il consenso viene richiesto in modo chiaro e separatamente da altri punti?	
Il consenso è formulato in modo facilmente comprensibile per l'interessato?	
Il linguaggio utilizzato per richiedere il consenso è chiaro e semplice?	
Le informazioni riferite al trattamento sono fornite prima di richiedere il consenso?	
Il consenso può essere revocato con la stessa facilità con cui viene prestato?	
All'interessato sono offerti strumenti per poter revocare il consenso in qualsiasi momento?	
Il consenso è totalmente libero?	

CONSENSO DEI MINORENNI PER I SERVIZI DELLA SOCIETA' DELL'INFORMAZIONE

Per servizi forniti a minori di 14 anni, viene richiesto il consenso al genitore o a chi ne ha la tutela?	
Viene verificato che il consenso sia stato effettivamente fornito dai genitori / tutori del minore?	

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI

Vengono trattati dati particolari solamente quando sussistono le eccezioni normative?	
Qualora il trattamento si basi sul consenso, questo è esplicito ed il trattamento non espressamente vietato da disposizioni normative?	
Il trattamento è necessario per adempiere degli obblighi o esercitare diritti specifici nell'ambito del diritto del lavoro e della sicurezza nella misura in cui ciò è stabilito dalle vigenti norme di legge?	
Il trattamento è necessario per adempiere degli obblighi o esercitare diritti specifici nell'ambito del diritto del lavoro e della sicurezza nella misura in cui ciò è stabilito da un contratto collettivo legalmente vincolante?	
Il trattamento è necessario per proteggere gli interessi vitali di una persona che non è fisicamente o legalmente capace di conferire il proprio consenso?	
Il trattamento riguarda membri attuali, ex membri o persone che mantengono contatti regolari con enti senza scopo di lucro (ad esempio operanti in campo politico, filosofico, religioso o sindacale) nell'ambito delle proprie attività legittimamente svolte?	
Il trattamento viene effettuato nell'ambito delle attività legittime e con garanzie adeguate; i dati acquisiti non vengono comunicati a terzi senza il consenso degli interessati.	
Vengono trattati dati che sono manifestamente resi pubblici dall'interessato.	
Il trattamento è necessario per l'esercizio o la difesa dei diritti.	
Il trattamento è necessario ai fini della medicina preventiva o del lavoro, della valutazione della capacità lavorativa del lavoratore, della diagnosi medica, della fornitura di assistenza o trattamento sanitario o sociale, o della gestione di sistemi e servizi di assistenza sanitaria e sociale.	
Il trattamento è necessario per motivi di interesse pubblico nel campo della salute pubblica sulla base di norme di legge che prevedono misure appropriate e specifiche per proteggere i diritti e le libertà della persona interessata, in particolare il segreto professionale.	

il trattamento è necessario per scopi di archiviazione nell'interesse pubblico, per scopi di ricerca scientifica o storica o per scopi statistici sulla base di norme di legge.	
Il trattamento viene effettuato nel rispetto delle condizioni relative al trattamento dei dati genetici, biometrici o relativi alla salute, come stabilito dalle normative nazionali.	

TRATTAMENTO DI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI

I dati sono trattati sotto il controllo delle autorità pubbliche.	
Il trattamento è autorizzato da vigenti norme legislative.	
Il registro completo delle condanne penali è tenuto sotto il controllo delle autorità pubbliche.	

TRATTAMENTI CHE NON RICHIEDONO IDENTIFICAZIONE

Le informazioni aggiuntive sono conservate al fine di identificare la persona interessata quando le finalità non richiedono tale identificazione.	
Ulteriori informazioni sono raccolte e/o trattate al fine di identificare la persona interessata quando le finalità non richiedono tale identificazione.	
È dimostrato che i dati anonimizzati non possono essere utilizzati per identificare gli interessati.	
I dati vengono cancellati quando la persona interessata viene identificata.	

DIRITTI DEGLI INTERESSATI. TRASPARENZA DELLE INFORMAZIONI

Sono stati implementati dei meccanismi per fornire alla persona interessata tutte le informazioni relative al trattamento.	
I meccanismi informativi vengono seguiti anche in caso di dati non raccolti direttamente presso l'interessato?	
Le informazioni sono fornite in forma concisa, trasparente e comprensibile.	
Le informazioni sono fornite in un linguaggio chiaro e semplice	
Le informazioni riferite al trattamento di dati personali sono fornite per iscritto o con altri mezzi, compresi i mezzi elettronici.	
L'esercizio dei diritti dell'interessato è facilitato / agevole	
Le richieste di esercizio dei diritti sono trattate anche se il trattamento non richiede l'identificazione, a meno che l'interessato non possa essere identificato.	
L'interessato riceve riscontro entro un mese dal ricevimento della domanda.	
Qualora sia necessario prolungare il tempo di riscontro alla richiesta dell'interessato, all'interessato viene comunque segnalata l'eventualità entro un mese, indicando il motivo del ritardo.	
Gli interessati possono esercitare i loro diritti tramite canali elettronici.	
All'interessato viene fornito riscontro circa le motivazioni in base alle quali si ritiene lecito il trattamento	
L'esercizio dei diritti è gratuito	
In caso di dubbi sull'identità della persona che esercita i diritti, vengono richieste informazioni per accertarsi che non vengano comunicati dati personali a soggetti non aventi diritto.	

RESPONSABILITA' DEL TITOLARE DEL TRATTAMENTO

La natura, la portata, il contesto e gli scopi del trattamento sono presi in considerazione per garantire e dimostrare che il trattamento è conforme al GDPR.	
I rischi di diversa probabilità e gravità per i diritti e le libertà delle persone fisiche sono presi in considerazione.	
Vengono attuate misure tecniche e organizzative appropriate	
Le misure sono riviste e aggiornate se necessario.	
Sono state elaborate policy di protezione dei dati.	
Le policy di protezione dei dati sono applicate	

PROTEZIONE DEI DATI PER PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

Le misure tecniche e organizzative appropriate sono analizzate prima di determinare i mezzi di trattamento.	
Le misure tecniche e organizzative appropriate per rispettare il GDPR sono prese in considerazione durante la progettazione del trattamento.	
Durante il trattamento, si applicano le misure che sono state determinate	
Durante il trattamento si controlla l'efficacia delle misure applicate.	
Vengono attuate misure tecniche e organizzative appropriate per garantire che, di default, vengano trattati solo i dati necessari per ogni scopo.	
Le misure tecniche e organizzative sono attuate tenendo conto della quantità di dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.	
Le misure garantiscono che, per default, i dati non sono accessibili a un numero indeterminato di persone fisiche, senza l'intervento del personale.	

CONTITOLARI DEL TRATTAMENTO

Le rispettive responsabilità delle parti contitolari per il rispetto degli obblighi imposti dal GDPR sono state determinate in modo trasparente e reciprocamente concordato.	
L'accordo stabilisce i rispettivi obblighi per la fornitura di informazioni alla persona interessata	
L'accordo tra i contitolari riflette i rispettivi ruoli e relazioni di entrambi in relazione ai soggetti dei dati.	
Gli aspetti essenziali dell'accordo sono disponibili su richiesta.	

RESPONSABILI DEL TRATTAMENTO

Vengono scelti i fornitori che offrono garanzie sufficienti secondo i requisiti del GDPR e garantiscono la protezione dei diritti dell'interessato	
Il responsabile non si avvale di altro responsabile senza autorizzazione del titolare del trattamento	
Il trattamento da parte del responsabile del trattamento è regolato da un contratto o da un altro atto giuridico vincolante secondo le norme di legge.	
Il contratto stabilisce l'oggetto, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di persone interessate, nonché gli obblighi e i diritti del responsabile del trattamento.	

Il contratto stabilisce che i dati personali sono trattati solo su istruzioni documentate del responsabile del trattamento.	
Il contratto garantisce che le persone autorizzate a trattare i dati personali si sono impegnate a rispettare la riservatezza o sono soggette a un obbligo di riservatezza di natura legale	
Il contratto prevede che il responsabile assista nel rispondere alle richieste di esercizio dei diritti degli interessati.	
Il contratto prevede la cancellazione o la restituzione dei dati personali al termine della fornitura dei servizi, e la cancellazione delle copie esistenti, a meno che non sia richiesta la conservazione dei dati personali.	
Il contratto prevede che il responsabile metta a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi stabiliti, così come per permettere e assistere i controlli e le ispezioni da parte del titolare del trattamento o di un altro verificatore da questi autorizzato.	
Il contratto prevede che se il responsabile del trattamento si avvale di un altro responsabile per svolgere determinate attività di trattamento per conto del responsabile del trattamento, gli stessi obblighi di protezione dei dati sono imposti a quest'ultimo come quelli stipulati nel contratto, per contratto o altro atto giuridico stabilito dalla legge.	
Il contratto è scritto	
L'accesso ai dati avviene solo su istruzione del responsabile del trattamento.	

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Viene tenuto un registro delle attività di trattamento	
Il registro contiene il nome e i dati di contatto del titolare del trattamento e, se del caso, del contitolare, del rappresentante del titolare e del responsabile della protezione dei dati.	
Il registro stabilisce le finalità del trattamento	
Contiene una descrizione delle categorie di interessati e delle categorie di dati personali	
Il registro elenca le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari in paesi terzi o organizzazioni internazionali.	
Il registro raccoglie i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione di tale paese terzo o organizzazione internazionale	
Sono inclusi i termini previsti per la cancellazione dei dati personali	
Il registro include una descrizione generale delle misure tecniche e organizzative adeguate al rischio delle operazioni di trattamento.	

SICUREZZA DEL TRATTAMENTO

Nel determinare le misure da applicare, si tiene conto dello stato dell'arte, dei costi di attuazione e della natura, della portata, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.	
Vengono attuate misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio.	
Sono state incluse misure per assicurare la continuità della riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di elaborazione.	
Sono state previste misure per garantire la capacità di ripristinare rapidamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico.	
Esiste un processo di verifica, valutazione e accertamento regolare dell'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento.	

I rischi presentati dal trattamento per distruzione, perdita o modifica accidentale o illecita dei dati personali trattati sono stati presi in considerazione nella valutazione del livello di sicurezza implementato	
Sono state prese misure per garantire che le persone autorizzate ad accedere ai dati li trattino solo a seguito di specifica istruzione.	

NOTIFICA DELLE VIOLAZIONI DELLA SICUREZZA DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO

Esiste una procedura per identificare e gestire le violazioni della sicurezza.	
Esiste una procedura che obbliga i responsabili del trattamento a notificare al titolare del trattamento le violazioni non appena ne vengono a conoscenza.	
Esiste una procedura di notifica all'autorità di controllo entro 72 ore.	
Esiste una procedura per documentare i motivi per cui non è possibile notificare entro 72 ore	
Esiste una procedura per fornire informazioni in modo graduale quando non è possibile fornirle simultaneamente.	
Qualsiasi violazione della sicurezza dei dati personali è documentata.	
La documentazione include i fatti correlati, i loro effetti e le azioni correttive adottate	
La procedura di notifica è stata verificata per garantirne il funzionamento	

COMUNICAZIONE DI UNA VIOLAZIONE ALL'INTERESSATO

Esiste una procedura per comunicare la violazione senza ritardi ingiustificati, quando è probabile che essa rappresenti un rischio elevato per i diritti e le libertà.	
La comunicazione all' interessato viene effettuata in un linguaggio chiaro e semplice, descrivendo la natura della violazione.	

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Quando un trattamento di dati personali può comportare un rischio elevato per i diritti e le libertà delle persone, viene svolta una PIA prima che questo abbia inizio.	
Una PIA viene effettuata prima del trattamento su larga scala di categorie particolari di dati o di dati relativi a condanne penali e reati.	
Una PIA è condotta prima di iniziare il trattamento che comporta la sorveglianza sistematica su larga scala di un'area accessibile al pubblico.	
Una PIA viene effettuata sui trattamenti inclusi nell'elenco pubblicato dall'autorità di controllo.	
La PIA include una descrizione sistematica delle operazioni di trattamento previste e delle finalità del trattamento, e se del caso l'interesse legittimo perseguito	
Comprende una valutazione della necessità e della proporzionalità delle operazioni di trattamento in relazione al loro scopo.	
La PIA include una valutazione dei rischi per i diritti e le libertà	
Include le misure previste per dimostrare la conformità con il GDPR, tenendo conto dei diritti e degli interessi legittimi degli interessati e di altre persone coinvolte.	
Include misure per mitigare i rischi e garantire la protezione dei dati.	
La PIA viene riesaminata ogni volta che è necessario e ogni volta che c'è un cambiamento nei rischi posti dalle operazioni di trattamento.	

L'autorità di controllo viene consultata prima del trattamento quando una PIA mostra che il trattamento comporterebbe un rischio elevato se non venissero adottate misure di attenuazione.	
Le rispettive responsabilità delle persone coinvolte nel trattamento sono riportate nella consultazione con l'autorità di controllo.	
Vengono fornite informazioni sulle finalità e i mezzi del trattamento previsti nella consultazione	
Vengono fornite informazioni sulle misure e le garanzie in atto per proteggere i diritti e le libertà degli interessati.	
Vengono forniti i dati di contatto del responsabile della protezione dei dati.	
In caso di consultazione, vengono fornite tutte le informazioni supplementari richieste dall'autorità di controllo.	

RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD O DPO)

Un DPO è stato nominato laddove richiesto dalla legge.	
Il DPO è stato nominato sulla base della sua professionalità, conoscenza e competenza nel campo.	
I dati di contatto del DPO sono resi conoscibili agli interessati e l'identità del DPO è stata comunicata all'autorità di controllo.	
Si assicura che il DPO sia coinvolto in modo appropriato e tempestivo in tutte le questioni relative alla protezione dei dati personali.	
Viene dato sostegno al DPO nello svolgimento dei propri compiti	
Il DPO dispone dei mezzi necessari per l'esecuzione delle sue funzioni, l'accesso ai dati personali e le operazioni di trattamento.	
Qualora il DPO sia interno, gli vengono fornite le risorse necessarie per mantenere le sue competenze.	
Si assicura che il DPO non riceva alcuna istruzione per quanto riguarda l'esercizio delle sue funzioni.	
Il DPO non può essere licenziato o sanzionato per aver svolto i suoi compiti.	
Il DPO riferisce direttamente ai vertici del titolare o del responsabile del trattamento.	
Il RPD risponde alle richieste degli interessati	
Se il DPO svolge altre funzioni, si assicura che esse non diano luogo a un conflitto di interessi.	
Tra le funzioni svolte dal RPD vi sono anche quelle di informare, assistere e formare il personale in merito ai propri obblighi.	
Il DPO coopera e funge da punto di contatto con l'autorità di controllo.	

TRASFERIMENTI DI DATI PERSONALI A PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

I trasferimenti vengono effettuati verso paesi o organizzazioni internazionali dichiarati dalla Commissione Europea come aventi un adeguato livello di protezione.	
La validità delle decisioni di adeguatezza della Commissione europea è monitorata.	
I trasferimenti sono effettuati mediante garanzie adeguate che forniscono alle parti interessate diritti concretamente azionabili.	
Esiste uno strumento giuridico vincolante ed esecutivo tra autorità o enti pubblici	
Ci sono regole aziendali vincolanti	
Esistono clausole standard di protezione dei dati adottate dalla Commissione.	

Esistono clausole standard di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione.	
C'è un codice di condotta unitamente ad impegni vincolanti ed esecutivi nel paese terzo per implementare salvaguardie adeguate.	
C'è un meccanismo di certificazione associato a impegni vincolanti ed esecutivi nel paese terzo che permette l'applicazione di salvaguardie adeguate.	
Ci sono clausole contrattuali che richiedono l'approvazione preventiva dell'autorità di vigilanza.	
Ci sono accordi amministrativi tra le autorità pubbliche e gli enti pubblici che incorporano disposizioni che includono diritti effettivi e applicabili per le parti interessate	
I trasferimenti internazionali avvengono in assenza di una decisione di adeguatezza della Commissione europea e di garanzie adeguate	
Il consenso esplicito dell'interessato è disponibile e lui/lei è stato informato dei possibili rischi.	
Sono necessari per l'esecuzione di un contratto con l'interessato o per l'esecuzione di misure precontrattuali adottate su richiesta dell'interessato.	
Sono necessari per la formulazione, l'esercizio o la difesa dei diritti.	
Sono necessari per la protezione degli interessi vitali della persona interessata o di altre persone, quando la persona interessata non è in grado di dare il consenso	
In caso di interessi legittimi cogenti, il trasferimento riguarda un numero limitato di soggetti e non è ripetitivo	
Tutte le circostanze prevalenti sono state valutate e sono state fornite garanzie appropriate.	
L'autorità di vigilanza è stata informata	

HAI DUBBI O DOMANDE? ECCO DI SEGUITO I NOSTRI CONTATTI

Effizient Srl, via Galvani 6/A 39100 Bolzano (BZ)
Tel. 0471 / 053 533
E-mail info@effizient.it
Web: www.effizient.it
LinkedIn https://it.linkedin.com/company/effizient-srl-gmbh