Direttiva sulla protezione dati UE

Mercedes-Benz

Indice

1 Finalità della direttiva

Il Mercedes-Benz Group tutela i diritti di protezione dei dati personali nell'ambito della sua responsabilità sociale.

In alcuni Paesi e regioni, come l'Unione Europea, il legislatore ha definito standard per la protezione dei dati delle persone fisiche (“dati personali”), compresa la condizione che tali dati possono essere trasmessi ad altri Paesi solo se la legge applicabile nel luogo di destinazione garantisce un livello adeguato di protezione dei dati.

La presente Direttiva sulla protezione dati UE definisce standard uniformi e adeguati per la protezione dei dati all'interno del Gruppo relativamente:
- (a) al trattamento di dati personali in regioni come l'UE/lo Spazio economico europeo (SEE) (di seguito definiti collettivamente “UE/SEE”) e
- (b) alla trasmissione transfrontaliera di dati personali a società del Gruppo esterne all'UE/SEE (compreso il trattamento successivo in tali Paesi).

A tal fine, la presente direttiva stabilisce regole vincolanti per il trattamento di dati personali provenienti dall'UE/SEE all'interno del Mercedes-Benz Group. Dette regole forniscono garanzie adeguate per la protezione dei dati personali all'esterno dell'UE/SEE e rappresentano norme vincolanti d'impresa (cosiddette “BCR - Binding Corporate Rules”) per il Mercedes-Benz Group.

2 Ambito di applicabilità

La presente Direttiva sulla protezione dati UE è valida per Mercedes-Benz Group AG, per le società controllate del Gruppo (di seguito società del Gruppo) nonché per i rispettivi dipendenti e membri degli organi amministrativi. "Controllo" in questo senso significa che Mercedes-Benz Group AG, direttamente o indirettamente, a seguito del voto di maggioranza, di una quota maggioritaria nella direzione aziendale o di un accordo, può esigere il recepimento della presente direttiva.

La direttiva si applica ai processi di trattamento dei dati personali completamente o parzialmente automatizzati, nonché al trattamento manuale in sistemi di archiviazione, fatto salvo un ambito di applicabilità più ampio se previsto dalla legislazione nazionale. In Germania la direttiva si applica anche a tutti i dati dei dipendenti[1] in formato cartaceo.
La direttiva si applica al trattamento di dati personali:
- (a) provenienti da società del Gruppo e dalle relative controllate aventi sede nell'UE/SEE o in un altro Paese al quale può essere estesa la presente direttiva (“società con sede nell'UE/SEE”),
- (b) provenienti da società del Gruppo aventi sede al di fuori dell'UE/SEE, se offrono beni o servizi a persone fisiche all'interno dell'UE/SEE e/o monitorano il comportamento di persone fisiche all'interno dell'UE/SEE (“società di Paesi terzi con offerte per l'UE/SEE”) o
- (c) provenienti da società del Gruppo aventi sede al di fuori dell'UE/SEE, se hanno ricevuto dati personali direttamente o indirettamente da società soggette alla direttiva conformemente al punto a) o b), o se detti dati sono stati ad esse divulgati (“società di Paesi terzi che ricevono dati dall'UE/SEE”).

[1] Per agevolare la lettura della presente direttiva, il testo impiega solo la forma maschile dei pronomi riferiti a persone fisiche. Tutte le declinazioni maschili includono sempre tutti gli individui, indipendentemente dall'identità di genere.

Nel proseguo della presente direttiva il trattamento al di fuori dell'UE/SEE è definito “trattamento in un Paese terzo”.

Le società del Gruppo che partecipano al trattamento da parte di società di Paesi terzi o che ne sono soggette sono elencate nell'altra norma applicabile “Elenco delle società del Gruppo vincolate dalla Direttiva sulla protezione dati UE”.

La presente direttiva può essere estesa a Paesi non facenti parte dell'UE/SEE. Nei Paesi in cui la tutela dei dati delle persone giuridiche è equiparata a quella dei dati personali, la presente direttiva è valida in egual misura per i dati di persone giuridiche.

3 Carattere giuridico vincolante all'interno del Mercedes-Benz Group

Le disposizioni della presente direttiva sono vincolanti per tutte le società del Gruppo che operano nel suo ambito di applicabilità. Pertanto, oltre alla legislazione UE applicabile e alla normativa nazionale in tema di protezione dei dati, le società del Gruppo nonché i loro dirigenti e dipendenti sono responsabili del rispetto della presente direttiva.

Se non diversamente stabilito da prescrizioni legali, le società del Gruppo non sono legittimate ad adottare regolamenti che deroghino dalla presente direttiva.

4 Rapporto con gli obblighi di legge

La presente direttiva non sostituisce la legislazione UE né la normativa nazionale. Essa integra le leggi nazionali vigenti in materia di protezione dati.. Dette leggi devono prevalere laddove il rispetto della presente direttiva comporti una violazione del diritto nazionale. In assenza di una legislazione nazionale corrispondente, il contenuto della presente direttiva deve essere rispettato.

Qualora il rispetto della presente direttiva comporti una violazione della normativa nazionale, o qualora la normativa nazionale imponga disposizioni che si discostano dalla presente direttiva, occorre informare il Responsabile per la protezione dati del Gruppo e l'organizzazione centrale per la compliance ai fini del monitoraggio del diritto per la protezione dati. In caso di contrasto tra la normativa nazionale e la presente direttiva, il Responsabile per la protezione dati del Gruppo e l'organizzazione centrale per la compliance dovranno collaborare con la società del Gruppo interessata per trovare una soluzione fattibile che soddisfi le finalità della presente direttiva.

5 Principi generali del trattamento di dati personali

5.1 Liceità

I dati personali devono essere raccolti e trattati in modo legittimo e corretto. Il loro trattamento può avere luogo solo e nella misura in cui sussista un fondamento giuridico sufficiente per tale operazione. Questo obbligo vale anche per il trattamento dei dati tra le società del Gruppo. Il semplice fatto che entrambe le parti, ossia la società del Gruppo che trasmette i dati e quella che li riceve, facciano parte del Mercedes-Benz Group non costituisce tale fondamento giuridico.

Il trattamento di dati personali è legittimo se sussiste una delle seguenti circostanze di autorizzazione di cui al paragrafo 5.2 o 5.3. Tali circostanze di autorizzazione sono necessarie anche qualora la finalità del trattamento dei dati personali debba essere modificata rispetto a quella originale.

5.2 Fondamento giuridico per dati di clienti e partner commerciali

5.2.1 Trattamento dati ai fini di un rapporto contrattuale

I dati personali di potenziali clienti, clienti esistenti o partner commerciali possono essere trattati ai fini della costituzione, esecuzione e conclusione di un contratto. Quanto sopra comprende anche l'assistenza fornita al cliente o al partner commerciale nell'ambito del contratto, qualora essa sia in relazione ai fini del contratto.

Nella fase preliminare del contratto è ammesso il trattamento di dati personali per la formulazione di offerte, la preparazione di ordini di acquisto o la soddisfazione di altre richieste del potenziale cliente in riferimento alla stipulazione del contratto. Durante l'avviamento del rapporto contrattuale, i potenziali clienti possono essere contattati tramite i dati che hanno comunicato. In tal caso bisogna tenere conto di eventuali limitazioni espresse dai potenziali Clienti.

5.2.2 Trattamento dati a fini pubblicitari

Qualora l'interessato si rivolga a una società del Gruppo con una richiesta di informazioni (ad es. per l'invio di materiale informativo su un prodotto), il trattamento di dati finalizzato a soddisfare tale richiesta è ammesso. Le misure di fidelizzazione del Cliente o pubblicitarie richiedono ulteriori requisiti giuridici. L'elaborazione di dati personali a fini pubblicitari o di ricerche di mercato o di opinione è ammessa, nella misura in cui ciò sia compatibile con lo scopo per il quale i dati sono stati originariamente rilevati. L'interessato deve essere preventivamente informato dell'utilizzo dei suoi dati personali a fini pubblicitari. Laddove i dati personali vengano raccolti esclusivamente per scopi pubblicitari, la loro comunicazione da parte dell'interessato è facoltativa. L'interessato deve essere informato sul carattere facoltativo della comunicazione dei dati ai suddetti fini. Nell'ambito della comunicazione con il soggetto interessato si deve ottenere il consenso al trattamento dei suoi dati. Nel rilasciare il proprio consenso, l'interessato deve poter scegliere fra diversi canali di contatto disponibili, come ad esempio e-mail e telefono (consenso, vedi par. 5.2.3). Nel caso in cui il soggetto interessato si opponga all'utilizzo dei suoi dati a fini pubblicitari, il trattamento di queste informazioni a tale scopo non è ammesso e i dati devono essere bloccati. Inoltre bisogna attenersi ad eventuali ulteriori limitazioni prescritte in alcuni Paesi in merito al trattamento dei dati a fini pubblicitari.

5.2.3 Consenso al trattamento di dati

Il trattamento dei dati personali può avere luogo sulla base del consenso dell'interessato. Prima di rilasciare il consenso, l'interessato deve essere informato in conformità alla presente Direttiva sulla protezione dati UE. Per motivi di documentazione, la dichiarazione di consenso deve essere rilasciata di norma per iscritto o elettronicamente. In alcuni casi, ad es. in caso di consulenza telefonica, il consenso può essere fornito anche verbalmente. Il suo rilascio deve comunque essere documentato.

5.2.4 Trattamento di dati sulla base di autorizzazioni od obblighi giuridici

Il trattamento di dati personali è consentito anche quando le norme di legge del rispettivo Stato richiedono, presuppongono o ammettono l'elaborazione dei suddetti dati. Il tipo e la portata del trattamento dei dati devono essere necessari all'attività di trattamento dati legalmente autorizzata ed essere corrispondenti ai requisiti prescritti dalla legge.

5.2.5 Trattamento di dati sulla base del legittimo interesse

I dati personali possono essere trattati anche qualora ciò sia necessario al perseguimento di un legittimo interesse. Con legittimi interessi si intendono di norma interessi di carattere legale (ad es. riscossione di crediti esigibili) o commerciale (ad es. prevenzione di violazioni contrattuali). Il trattamento sulla base di un legittimo interesse non può avvenire se nel caso specifico gli interessi meritevoli di tutela dell'interessato prevalgono sul legittimo interesse al trattamento dei dati. Questo aspetto deve essere verificato caso per caso.

5.3 Base giuridica per i dati dei dipendenti

5.3.1 Trattamento di dati finalizzato al rapporto lavorativo

Ai fini del rapporto lavorativo è consentito il trattamento dei dati personali per la stipula, l'esecuzione e la conclusione del contratto di lavoro. Per decidere se instaurare un rapporto di lavoro è consentito trattare i dati personali dei candidati. Se il candidato è respinto, i suoi dati devono essere cancellati rispettando i termini di conservazione previsti, salvo il caso in cui il candidato abbia acconsentito al loro mantenimento per un processo di selezione futuro. Il consenso è necessario anche per l'utilizzo dei dati ai fini di ulteriori processi di selezione di candidati o prima dell'eventuale trasmissione ad altre società del Gruppo. Nel rapporto di lavoro esistente il trattamento dei dati deve essere sempre riferito alle finalità del contratto di lavoro, se non sussiste uno dei seguenti motivi di autorizzazione al trattamento dei dati personali.

Qualora nella fase di avviamento del rapporto di lavoro o nel corso del medesimo si dovesse rendere necessario il rilevamento di informazioni sul Collaboratore presso terzi, bisogna attenersi alle rispettive norme di legge nazionali. In caso di dubbio va richiesto il consenso dell'interessato, laddove permesso.

Per il trattamento di dati personali che rientrano nel contesto del rapporto di lavoro, ma che originariamente non attenevano all'instaurazione, all'esecuzione o alla conclusione del rapporto di lavoro deve sussistere una base giuridica secondo quanto elencato sotto (dati dei dipendenti).

5.3.2 Trattamento di dati sulla base di autorizzazioni od obblighi giuridici

Il trattamento di dati dei Collaboratori è consentito anche quando le norme di legge del rispettivo Stato richiedono, presuppongono o ammettono l'elaborazione dei suddetti dati. Il tipo e la portata del trattamento dei dati devono essere necessari all'attività di trattamento dati legalmente autorizzata ed essere corrispondenti ai requisiti prescritti dalla legge. Qualora sussista un margine di manovra giuridico, bisogna comunque tutelare gli interessi sensibili del Collaboratore.

5.3.3 Clausole dei contratti collettivi sul trattamento dei dati

Se un trattamento dati esula dalle finalità contrattuali, esso può comunque essere legittimo se ammesso da un contratto collettivo. Le clausole devono riguardare lo scopo specifico del trattamento dati richiesto e devono essere redatte entro i parametri del diritto nazionale e dell'UE.

5.3.4 Consenso al trattamento di dati

I dati dei dipendenti possono essere trattati sulla base del consenso dell'interessato. Le dichiarazioni di consenso devono essere rilasciate spontaneamente. Il rifiuto al consenso non deve comportare sanzioni. Il consenso non rilasciato spontaneamente non è valido. Per motivi di documentazione, la dichiarazione di consenso deve essere rilasciata di norma per iscritto o elettronicamente. Qualora in via eccezionale le circostanze non lo consentano, il consenso può essere rilasciato verbalmente. In ogni caso il rilascio del consenso deve essere regolarmente documentato. Prima di rilasciare il consenso, l'interessato deve essere informato in conformità alla presente Direttiva sulla protezione dati UE.

5.3.5 Trattamento di dati sulla base del legittimo interesse

I dati dei dipendenti possono essere trattati anche qualora ciò sia necessario al perseguimento di un legittimo interesse di una società del Gruppo. Con legittimi interessi si intendono di norma interessi di carattere legale (ad es. per accertare, esercitare o difendere un diritto) o commerciale (ad es. accelerazione di processi aziendali, valutazione di società). Prima del trattamento dei dati è necessario stabilire se sussistono interessi meritevoli di tutela. Il trattamento dei dati personali è ammesso per il perseguimento del legittimo interesse, purché gli interessi meritevoli di tutela del dipendente non prevalgano sull'interesse nel trattamento.

I provvedimenti di controllo che richiedono il trattamento dei dati del dipendente al di là dell'esecuzione del rapporto di lavoro (ad es. controlli delle prestazioni) non possono essere adottati, salvo il caso in cui sussista un obbligo di legge o un motivo giustificato. Anche in presenza di un motivo legittimo deve comunque essere verificata la proporzionalità del provvedimento di controllo. Gli interessi legittimi della società del Gruppo allo svolgimento del provvedimento di controllo (ad es. il rispetto delle norme di legge e di regole interne aziendali) devono essere valutati a fronte di un possibile interesse di tutela che il dipendente oggetto del provvedimento potrebbe avere nell'esclusione di tale provvedimento. I provvedimenti possono essere adottati solo se appropriati per il caso specifico. L'interesse giustificato della società del Gruppo e i possibili interessi sensibili del Collaboratore devono essere stabiliti e documentati prima dell'adozione di qualsiasi provvedimento. Inoltre bisogna tenere conto di eventuali ulteriori requisiti prescritti dalle norme vigenti (ad es. diritti di cogestione della rappresentanza sindacale e diritti all'informazione degli interessati).

5.4 Trattamento di dati particolarmente sensibili

Il trattamento dei dati personali particolarmente sensibili deve essere espressamente consentito o prescritto dalla legislazione nazionale. . Il trattamento di tali dati da parte della società del Gruppo può essere consentito, in particolare, se l'interessato ha fornito il suo consenso esplicito, se il trattamento è necessario per far valere, esercitare o difendere un diritto nei confronti dell'interessato o se è necessario per permettere al titolare del trattamento di adempiere i propri diritti e doveri nel campo del diritto del lavoro.

Laddove si preveda il trattamento di dati personali particolarmente sensibili, il Responsabile per la protezione dati del Gruppo deve essere informato anticipatamente.

5.5 Decisioni automatizzate (possibilmente inclusa la profilazione)

L'interessato può essere soggetto a una decisione completamente automatizzata che potrebbe avere un impatto giuridico o analogamente negativo su di lui soltanto se è necessario alla stipulazione o all'esecuzione di un contratto, oppure se l'interessato ha fornito il suo consenso. Questa decisione automatizzata può includere in alcuni casi la profilazione, ossia il trattamento di dati personali con il quale si valutano le caratteristiche della personalità specifica (ad es. l'affidabilità creditizia). In questo caso è necessario comunicare all'interessato la circostanza e l'esito della decisione individuale automatizzata e fornirgli l'opportunità di far eseguire una verifica individuale da un titolare del trattamento.

5.6 Dovere di informazione/trasparenza

Il reparto responsabile deve fornire all'interessato informazioni sulle finalità e sulle circostanze del trattamento dei suoi dati personali, conformemente all'art. 13 e 14 GDPR. Se i dati non rientrano nell'ambito di applicazione del GDPR, le informazioni vengono fornite in conformità con la legge nazionale applicabile. Le informazioni devono essere fornite in forma precisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Occorre rispettare i requisiti posti dal Responsabile della protezione dati del Gruppo e per la compliance dati. Queste informazioni devono essere fornite nel momento in cui i dati personali vengono raccolti per la prima volta. Se la società del Gruppo riceve i dati personali da terzi, deve informarne l'interessato entro un lasso di tempo ragionevole dopo la ricezione dei dati, salvo il caso in cui:

- l'interessato disponga già di tali informazioni o
- sia impossibile o
- estremamente difficile fornire tali informazioni.

5.7 Limitazione della finalità

I dati personali possono essere trattati solo per la finalità legittima definita prima della raccolta dei dati stessi. Modifiche a posteriori della finalità del trattamento sono consentite solo nella misura in cui il trattamento sia compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti.

5.8 Minimizzazione dei dati

Il trattamento dei dati personali deve essere limitato, sia quantitativamente sia qualitativamente, a quanto necessario alle finalità per le quali i dati sono legittimamente trattati. Questo requisito deve essere tenuto in considerazione durante la fase iniziale di raccolta dei dati. Se la finalità lo permette e l'onere è proporzionato alla finalità perseguita, si devono utilizzare dati anonimi o statistici.

5.9 Esattezza dei dati

I dati personali archiviati devono essere oggettivamente esatti e, se necessario, aggiornati. L'unità funzionale responsabile deve adottare misure ragionevoli per cancellare, rettificare, integrare o aggiornare i dati inesatti o incompleti.

5.10 Riservatezza fin dalla progettazione e protezione dei dati per impostazione predefinita

Il principio della “protezione dei dati fin dalla progettazione” mira a garantire che le unità funzionali definiscano strategie interne tenendo conto dello stato dell'arte e adottino provvedimenti per integrare i principi di protezione dei dati nelle specifiche e nell'architettura di modelli di business/processi e di sistemi IT per il trattamento dei dati fin dal principio, ossia già nella fase di ideazione e progettazione tecnica. In conformità al principio della “riservatezza fin dalla progettazione”, le procedure e i sistemi per il trattamento dei dati personali devono essere configurati in modo tale che le loro impostazioni predefinite siano limitate al trattamento dati necessario alla specifica finalità (principio della “protezione dei dati per impostazione predefinita”). Tale obbligo vale per la portata del trattamento, il periodo di conservazione e l'accessibilità. Ulteriori provvedimenti potrebbero includere:

- la pseudonimizzazione dei dati personali quanto prima possibile
- la trasparenza sulle funzioni e sul trattamento dei dati personali
- la possibilità per gli interessati di decidere sul trattamento dei loro dati personali
- la possibilità di creare e migliorare le funzioni di sicurezza da parte dei gestori di procedure o sistemi.

Ogni società del Gruppo adotta e mantiene provvedimenti tecnici e organizzativi appropriati per l'intera durata delle attività di trattamento dati, al fine di garantire che i suddetti principi siano sempre rispettati.

5.11 Cancellazione e trasformazione in forma anonima

I dati personali possono essere archiviati solo per il tempo necessario alla finalità per la quale sono stati trattati. Ciò significa che i dati personali devono essere cancellati o resi anonimi non appena lo scopo del loro trattamento è stato raggiunto o viene meno, purché non sussistano ulteriori obblighi di conservazione o di certificazione. I responsabili delle singole procedure devono garantire l'attuazione delle operazioni di cancellazione e trasformazione in forma anonima per le loro procedure. Ogni sistema deve disporre di una funzione di cancellazione manuale o automatizzata. Le richieste di cancellazione da parte degli interessati mediante cancellazione o rimozione degli identificatori personali devono essere tecnicamente attuabili nei sistemi. I requisiti imposti da Mercedes-Benz Group AG per l'esecuzione delle operazioni di cancellazione (come strumenti software, documenti per l'implementazione delle operazioni di cancellazione, requisiti di documentazione) devono essere rispettati.

5.12 Sicurezza del trattamento

I dati personali vanno protetti dall'accesso non autorizzato e dal trattamento o trasferimento illeciti, nonché dalla perdita, dall'alterazione o dalla distruzione accidentali. Prima di introdurre nuovi metodi di trattamento dei dati, in particolare nuovi sistemi IT, è necessario definire e attuare misure tecniche e organizzative finalizzate alla protezione dei dati personali. Queste misure devono tenere conto dello stato dell'arte, dei rischi del trattamento e della necessità di proteggere i dati.

Le misure tecniche e organizzative attinenti alla protezione dei dati devono essere documentate dal titolare del trattamento nell'ambito della Valutazione dell'impatto sulla protezione dei dati e del Registro delle attività di trattamento.

In particolare, l'unità funzionale responsabile deve consultarsi con il suo Business Information Security Officer (BISO), il suo Information Security Officer (ISO) e la sua Rete per la protezione dati. I requisiti delle misure tecniche e organizzative per la protezione dei dati personali fanno parte della Gestione della sicurezza delle informazioni aziendali e vanno costantemente aggiornati sulla base degli sviluppi tecnici e dei cambiamenti organizzativi.

5.13 Inoltro all'esterno del Mercedes-Benz Group

La trasmissione dei dati personali a destinatari interni o esterni alle società del Gruppo è soggetta ai requisiti di autorizzazione per il trattamento dei dati personali di cui al presente paragrafo 5. Il destinatario dei dati deve essere vincolato all'utilizzo dei medesimi esclusivamente per gli scopi prestabiliti.

In caso di trasmissione transfrontaliera dei dati personali (incluso l'accesso consentito da un altro Paese) occorre soddisfare i requisiti nazionali attinenti al trasferimento di dati personali all'estero. In particolare, i dati personali provenienti dall'UE/SEE possono essere trattati all'esterno delle società del Gruppo in un Paese terzo solo se il destinatario è in grado di dimostrare di disporre di un livello di protezione dati conforme alla presente direttiva. Strumenti idonei a tale scopo possono essere:

- accordo su clausole contrattuali standard dell'UE,
- partecipazione del destinatario a un sistema di certificazione accreditato dall'UE, atto a garantire un livello adeguato di protezione dei dati, o
- riconoscimento di regole aziendali vincolanti del destinatario al fine di garantire un livello adeguato di protezione dei dati da parte delle autorità di controllo responsabili.

La trasmissione di dati personali a un'autorità non deve essere effettuata in modo massiccio, sproporzionato e indiscriminato, e non deve superare il limite di ciò che è necessario in una società democratica. In caso di conflitto tra questi requisiti e quelli posti dalle autorità pubbliche, Mercedes-Benz Group AG collaborerà con la società del Gruppo responsabile per individuare una soluzione pratica che soddisfi la finalità della presente direttiva (paragrafo 14.3).

Tutti gli obblighi elencati al paragrafo 5 sono diritti del terzo beneficiario l'interessato.

6 Valutazione dell'impatto sulla protezione dei dati

In fase di introduzione di nuovi processi di trattamento, o in caso di modifica significativa a un processo esistente prima del trattamento, in particolare attraverso l'uso di nuove tecnologie, le società del Gruppo devono valutare se tale trattamento comporta un rischio elevato per la sfera privata dell'interessato. Occorre prendere in considerazione la natura, la portata, il contesto e la finalità del trattamento dei dati. Nell'ambito dell'analisi dei rischi, l'unità funzionale responsabile effettua una valutazione dell'impatto del trattamento pianificato sulla protezione dei dati personali (Valutazione dell'impatto sulla protezione dei dati). Se a seguito della Valutazione dell'impatto sulla protezione dei dati e dell'adozione di provvedimenti volti a ridurre al minimo i rischi sussiste un rischio elevato per i diritti e le libertà degli interessati, se ne deve informare il Responsabile della protezione dati del Gruppo, affinché possa rivolgersi all'autorità di controllo per la protezione dati competente. Occorre rispettare le direttive definite da Mercedes-Benz Group AG per l'esecuzione di tale valutazione (ad esempio strumenti software, istruzioni sull'effettuazione della valutazione).

7 Documentazione delle procedure di trattamento dei dati

Ogni società del Gruppo deve documentare in un registro delle attività di trattamento le procedure nelle quali vengono trattati i dati personali. Il registro delle attività di trattamento deve essere redatto in forma scritta, compreso anche il formato elettronico, e su richiesta deve essere messo a disposizione dell'autorità di controllo per la protezione dati. Occorre rispettare le direttive definite da Mercedes-Benz Group AG per la documentazione (come strumenti software, istruzioni per la documentazione).

8 Trattamento per conto del titolare del trattamento

8.1 Aspetti generali

Il trattamento per conto del titolare del trattamento ha luogo quando un responsabile del trattamento tratta i dati personali in qualità di fornitore di un servizio per conto e secondo le istruzioni del titolare del trattamento. In questi casi è necessario stipulare un accordo sul trattamento per conto del titolare del trattamento sia con responsabili esterni, sia tra società all'interno del Mercedes-Benz Group, secondo le disposizioni di legge vigenti (ad es. modello “Accordo sul trattamento per conto del titolare del trattamento”). Il titolare del trattamento si assume la piena responsabilità della correttezza del processo di trattamento dati.

Le disposizioni del paragrafo 8.3 si applicano anche a titolari del trattamento esterni che non siano società del Gruppo.

8.2 Direttive per titolari del trattamento

All'emissione di un ordine si devono osservare le seguenti direttive, la cui attuazione deve essere assicurata dall'unità funzionale competente:

- Il responsabile del trattamento deve essere selezionato in base alla sua idoneità a garantire le necessarie misure di sicurezza tecniche e organizzative.
- Si devono rispettare gli standard contrattuali per la protezione dei dati stabiliti dal Responsabile per la protezione dati del Gruppo.
- L'incarico deve essere conferito per iscritto o in forma elettronica. Nel conferimento devono essere documentate sia le istruzioni per il trattamento dei dati sia le responsabilità del titolare del trattamento e quelle del responsabile del trattamento.

Prima di iniziare il trattamento dei dati, il titolare del trattamento deve accertarsi mediante adeguata valutazione che il responsabile del trattamento rispetterà gli obblighi suddetti. Occorre rispettare le direttive stabilite da Mercedes-Benz Group AG al riguardo (ad esempio strumenti software, istruzioni per lo svolgimento della valutazione, modello di contratto). In particolare, il rispetto dei requisiti di sicurezza dei dati può essere dimostrato dal responsabile del trattamento presentando un'idonea certificazione. A seconda del livello di rischio del processo di trattamento dei dati, le verifiche devono essere ripetute a intervalli regolari durante il periodo contrattuale.

8.3 Direttive per responsabili del trattamento interni

Il responsabile del trattamento può trattare i dati personali solo nel rispetto delle istruzioni del titolare del trattamento.

I responsabili del trattamento possono conferire ad altre società del Gruppo o a terzi ("subincaricati") il compito di trattare i dati personali nel loro (sub)incarico solo previo consenso del titolare del trattamento. Tale consenso viene concesso solo se il responsabile del trattamento vincola il subincaricato – mediante contratto o altri strumenti giuridici vincolanti analoghi – ai medesimi obblighi di protezione dei dati ai quali è soggetto il responsabile del trattamento nei confronti della società del Gruppo e degli interessati in conformità alla presente direttiva. Il subincaricato è tenuto anche ad attuare adeguate misure di protezione di tipo tecnico e organizzativo. La forma del consenso e gli obblighi di informazione in caso di modifiche nel conferimento dell'incarico al subincaricato vanno regolati nel contratto di prestazione di servizi.

I responsabili del trattamento sono obbligati a garantire al titolare del trattamento un supporto adeguato nel rispettare le direttive di protezione dati applicabili a quest'ultimo, soprattutto fornendo tutte le informazioni necessarie. Quanto suddetto riguarda, in particolare, il rispetto

- dei principi generali per il trattamento, in conformità al paragrafo 5
- dei diritti degli interessati, in conformità al paragrafo 10
- dell'obbligo di notificare gli incidenti che riguardano la protezione dati, in conformità al paragrafo 12
- delle direttive per il titolare del trattamento e i responsabili del trattamento, in conformità al paragrafo 8
- e della gestione di richieste e indagini condotte dalle autorità di controllo.

Se norme applicabili o disposizioni legali impongono al responsabile del trattamento di effettuare il trattamento in modo contrario alle istruzioni del titolare del trattamento, oppure se tali disposizioni impediscono al responsabile del trattamento di adempiere i suoi obblighi previsti dalla presente direttiva o dall'accordo sul trattamento per conto del titolare del trattamento, il responsabile del trattamento deve informare immediatamente il suo titolare del trattamento, salvo il caso in cui la disposizione di legge in questione vieti tale notifica. Quanto suddetto si applica analogamente qualora il responsabile del trattamento non sia in grado di rispettare le istruzioni del titolare del trattamento per altre ragioni. In tal caso il titolare del trattamento ha il diritto di sospendere la trasmissione dei dati e/o di porre fine all'accordo sul trattamento per suo conto.

I responsabili del trattamento sono tenuti a notificare ai loro titolari del trattamento eventuali richieste vincolanti di comunicazione di dati personali ricevute da autorità pubbliche, purché tale notifica non sia vietata per altre ragioni.

Al termine della prestazione del servizio, il responsabile del trattamento deve cancellare o restituire – a discrezione del titolare del trattamento – tutti i dati personali forniti dal titolare del trattamento.

I responsabili del trattamento sono tenuti a informare immediatamente il titolare del trattamento e, se del caso, il cliente del titolare del trattamento circa rivendicazioni, richieste o reclami presentati dagli interessati.

I titolari del trattamento interni al Gruppo devono vincolare i responsabili del trattamento esterni anche al rispetto delle suddette regole.

Gli obblighi specifici del responsabile del trattamento nei confronti del titolare del trattamento sono diritti del terzo beneficiario per l'interessato.

9 Joint Controllership

Nel caso in cui più società del Gruppo definiscano congiuntamente i mezzi e gli scopi del trattamento dei dati personali (insieme a una o più parti terze, se presenti) (titolari del trattamento congiunti/ Joint Controller), le società devono stipulare un accordo che definisca i loro doveri e le loro responsabilità nei confronti dell'interessato di cui stanno trattando i dati. In tale ambito occorre attenersi ai modelli di contratto forniti dal Responsabile per la protezione dati del Gruppo.

10 Diritti applicabili per gli interessati

Tutti i diritti degli interessati e gli obblighi delle società del Gruppo elencati nel paragrafo 10 sono diritti del terzo beneficiario per l'interessato.

Alle richieste e ai reclami presentati in conformità al paragrafo 10 si deve fornire una risposta entro un mese. In considerazione della complessità e del numero di richieste, tale termine di un mese può essere esteso fino a un massimo di tre mesi, informandone l'interessato.

10.1 Diritti dell'interessato

L'interessato dal trattamento dati nell'UE/ SEE gode dei diritti di seguito elencati, esposti più dettagliatamente nella legislazione UE, nei confronti della società del Gruppo responsabile o, se la società del Gruppo corrisponde al responsabile del trattamento, nei confronti del titolare del trattamento.

- Il diritto di essere informato delle circostanze in cui i suoi dati personali sono stati trattati. Occorre rispettare i requisiti posti dal Responsabile per la protezione dati del Gruppo per tali informazioni.
- Il diritto di ottenere informazioni sulle modalità di trattamento dei suoi dati e sui diritti di cui gode in tal senso. Qualora, secondo il rispettivo diritto del lavoro vigente, sussistano specifici diritti alla visione dei documenti del datore di lavoro (ad es. documenti del personale), questi ultimi rimangono inalterati. Su richiesta, l'interessato può ricevere una copia dei suoi dati personali (eventualmente dietro compenso adeguato), purché a questo diritto non si oppongano interessi meritevoli di tutela di terzi.
- Il diritto alla rettifica o all'integrazione dei dati personali se sono inesatti o incompleti.
- Il diritto alla cancellazione dei suoi dati personali, qualora revochi il consenso o il fondamento giuridico non sussista più. Lo stesso diritto si applica nel caso in cui la finalità del trattamento dati non sussista più o cessi di essere applicabile per altre ragioni. Occorre rispettare il periodo di conservazione e gli interessi meritevoli di tutela che ne proibiscono la cancellazione.
- Il diritto alla limitazione del trattamento dei suoi dati se contesta la loro esattezza o se la società del Gruppo non ha più bisogno dei dati, mentre all'interessato sono necessari per i suoi diritti in sede giudiziaria. L'interessato può anche richiedere che la società del Gruppo limiti il trattamento dei suoi dati qualora la società debba altrimenti cancellare i dati o qualora stia verificando un'obiezione sollevata dall'interessato.
- Il diritto di ricevere in un formato digitale di uso comune i dati personali che lo riguardano e che ha fornito sulla base del consenso, o nell'ambito di un accordo stipulato con lui. Inoltre ha il diritto di trasmettere tali dati a terzi se il trattamento è stato effettuato con mezzi automatizzati e se la trasmissione è tecnicamente fattibile.
- Il diritto di opporsi in qualsiasi momento al trattamento dei dati per finalità di marketing diretto. Occorre garantire un sistema adeguato di gestione dei consensi e delle opposizioni.

- Il diritto di opporsi al trattamento dei dati personali effettuato sulla base legale di interessi prevalenti di una società del Gruppo o di terzi, per ragioni connesse alla sua particolare situazione personale. Tuttavia, questo diritto di opposizione non è valido se la società del Gruppo ha motivi cogenti per procedere al trattamento oppure se i dati sono trattati per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Se l'opposizione è legittima, i dati devono essere cancellati.

Inoltre, l'interessato è legittimato a far valere i suoi diritti nei confronti della società del Gruppo che importa i dati in un Paese terzo.

10.2 Procedura di reclamo

Gli interessati hanno il diritto di presentare reclamo al Responsabile della protezione dati del Gruppo se ritengono che la presente direttiva sia stata violata. Reclami di questo tipo possono essere presentati via e-mail.

La società del Gruppo con sede nell'UE/ SEE che esporta i dati deve assistere l'interessato i cui dati personali sono stati raccolti nell'UE/ SEE, per accertare i fatti e far valere i suoi diritti conformemente alla presente direttiva nei confronti della società del Gruppo che importa i dati.

Qualora l'interessato non concordi con la decisione della società del Gruppo sul rispetto delle disposizioni (o qualora non sia soddisfatto dell'operato della società), ha la facoltà di contestare tale decisione od operato esercitando i suoi diritti. A tal fine può rivolgersi all'autorità di controllo competente, in particolare nel Paese in cui risiede abitualmente, lavora oppure del luogo dove si è verificata la presunta violazione, o promuovere un'azione dinanzi a un tribunale (paragrafo 11.2). Ulteriori diritti e responsabilità previsti dalla legge restano inalterati.

11 Responsabilità e foro competente

11.1 Disposizioni sulla responsabilità

La società del Gruppo con sede nell'UE/SEE (“esportatore dei dati”) che ha inizialmente trasmesso i dati personali a una società del Gruppo con sede in un Paese terzo si assume la responsabilità di qualsiasi violazione della presente direttiva da parte di detta società del Paese terzo che riceve i dati dall'UE/SEE per il trattamento in Paesi terzi. Questa responsabilità include l'obbligo di porre rimedio a situazioni illecite e risarcire i danni materiali e immateriali causati dalla violazione della presente direttiva da parte di società del Gruppo provenienti da Paesi terzi.

L'esportatore dei dati è esonerato da tale responsabilità in tutto o in parte solo se è in grado di dimostrare che la società del Paese terzo che riceve i dati dall'UE/SEE non è responsabile dell'evento che ha causato il danno.

11.2 Foro competente

L'interessato può promuovere un'azione dinanzi alle autorità giurisdizionali nella sede del titolare del trattamento o del responsabile del trattamento oppure nel luogo in cui l'interessato risiede abitualmente.

L'interessato dal trattamento dei suoi dati personali che faccia valere una violazione della presente direttiva nell'ambito di un trattamento in Paesi terzi ha facoltà di intentare un'azione legale nell'UE/SEE sia nei confronti della società che importa i dati sia di quella che li esporta. Pertanto, l'interessato può presentare la presunta violazione e intentare la conseguente azione legale dinanzi al foro competente e alle autorità di controllo presso la sede del titolare del trattamento o la sua residenza abituale.

Le disposizioni sulla responsabilità e sul foro competente di questo paragrafo sono diritti del terzo beneficiario per l'interessato.

12 Notifica di incidenti che riguardano la protezione dati

In caso di potenziale violazione delle direttive per la sicurezza dei dati (“incidente nella protezione dei dati”), le società del Gruppo coinvolte hanno l'obbligo di indagare, informarsi e ridurre il danno. Un incidente nella protezione dei dati rappresenta una violazione dei dati personali se sussiste una violazione della sicurezza dei dati che causa illecitamente distruzione, alterazione, divulgazione o utilizzo non autorizzati dei dati personali. Quando la violazione dei dati personali può comportare un rischio per i diritti e le libertà di persone fisiche, l'autorità di controllo responsabile deve essere informata di tale violazione possibilmente entro 72 ore dal momento in cui la società del Gruppo ne è venuta a conoscenza. Inoltre gli interessati devono ricevere notifica di qualsiasi violazione dei loro dati personali che possa comportare un rischio elevato per i loro diritti e le loro libertà. I responsabili del trattamento ai sensi del paragrafo 8.2 sono obbligati a denunciare immediatamente gli incidenti nella protezione dei dati al titolare del trattamento.

Se si riscontra o si sospetta l'esistenza di un incidente nella protezione dei dati nell'ambito di responsabilità di una società del Gruppo, tutti i dipendenti sono tenuti a segnalarlo immediatamente in conformità al processo Information Security Incident Management. Occorre rispettare le direttive stabilite da Mercedes-Benz Group AG al riguardo (ad esempio strumenti software, istruzioni per la segnalazione).

Ogni violazione della protezione dati deve essere documentata e la relativa documentazione deve essere messa a disposizione dell'autorità di controllo su richiesta.

13 Organizzazione per la protezione dei dati e sanzioni

13.1 Responsabilità

I membri degli organi amministrativi delle società del Gruppo sono responsabili del trattamento dati nella loro area di competenza. Pertanto, devono assicurare l'osservanza dei requisiti di legge in tema di protezione dati e delle disposizioni contenute nella presente Direttiva sulla protezione dati UE (ad es. obblighi di denuncia alle autorità nazionali). Nell'ambito di responsabilità dei dirigenti rientra l'obbligo di garantire che siano poste in essere misure organizzative, personali e tecniche finalizzate a un trattamento dati conforme ai requisiti della protezione dati. Il rispetto di tali direttive è responsabilità dei dipendenti competenti. In caso di controlli sulla protezione dati da parte delle autorità competenti, il Responsabile Protezione Dati del Gruppo deve essere informato senza indugio.

13.2 Sensibilizzazione e formazione

I dirigenti devono assicurare che i loro dipendenti ricevano e partecipino ai corsi di formazione richiesti in tema di protezione dati, compreso il contenuto e la gestione della presente direttiva, qualora abbiano accesso costante o frequente a dati personali, prendano parte alla raccolta di dati o allo sviluppo di strumenti per il trattamento di dati personali. Occorre rispettare i requisiti posti dal Responsabile della protezione dati del Gruppo e per la compliance dati.

13.3 Organizzazione

Il Responsabile della protezione dati del Gruppo è indipendente da istruzioni interne relative all'esecuzione dei suoi incarichi. Deve garantire il rispetto della normativa nazionale e internazionale in tema di protezione dati. È responsabile della presente direttiva e ne controlla l'osservanza. Se le società del Gruppo desiderano far parte di un sistema di certificazione internazionale per norme vincolanti d'impresa in tema di protezione dei dati, devono concordare tale partecipazione con il Responsabile della protezione dati del Gruppo.

Il Responsabile della protezione dati del Gruppo è nominato dal Consiglio direttivo di Mercedes-Benz Group AG e viene supportato dal Consiglio direttivo nell'espletamento delle sue funzioni. Generalmente, le società del Gruppo con obbligo legale di nominare un responsabile della protezione dei dati designano il Responsabile della protezione dati del Gruppo. Il Responsabile della protezione dati del Gruppo riferisce direttamente al Consiglio direttivo di Mercedes-Benz Group AG e alla dirigenza della rispettiva società del Gruppo per la quale il Responsabile della protezione dati del Gruppo è stato nominato. Eventuali eccezioni devono essere concordate con il Responsabile Protezione Dati del Gruppo.

La commissione di vigilanza di Mercedes-Benz Group AG deve essere informata della relazione annuale del Responsabile della protezione dati del Gruppo, nell'ambito degli obblighi di notifica esistenti.

Qualsiasi interessato può rivolgersi al Responsabile per la protezione dati del Gruppo in qualsiasi momento per esprimere preoccupazioni, porre domande, richiedere informazioni o presentare reclami relativi a questioni di protezione o sicurezza dei dati. Se richiesto, preoccupazioni e reclami possono essere trattati in modo confidenziale.

Il Responsabile per la protezione dati del Gruppo può essere contattato ai seguenti recapiti:

Mercedes-Benz Group AG, Responsabile per la protezione dati del Gruppo, HPC E600,
70546 Stoccarda, Germania
E-mail: data.protection@mercedes-benz.com
Intranet: https://social.intra.corpintra.net/docs/DOC-71499

Il Mercedes-Benz Group ha anche istituito un'organizzazione per la compliance, descritta più dettagliatamente in regolamenti interni distinti. L'organizzazione per la compliance supporta e vigila sulle società del Gruppo rispetto alla compliance con la normativa sulla protezione dati. Definisce il contenuto della formazione sulla protezione dati e fissa i criteri per il gruppo di partecipanti.

13.4 Sanzioni

Il trattamento illecito di dati personali o altre violazioni della normativa sulla protezione dati possono essere perseguiti anche penalmente in molti Paesi e possono comportare richieste di risarcimento danni. Le violazioni di cui sono responsabili i singoli dipendenti possono comportare azioni disciplinari previste dalla normativa del lavoro. Le violazioni della presente direttiva sono sanzionate in conformità ai regolamenti interni.

13.5 Audit e controlli

L'osservanza della presente direttiva e della normativa sulla protezione dati applicabile viene verificata a livello di Gruppo con cadenza regolare, almeno una volta all'anno, mediante controlli basati sui rischi. Tali controlli sono eseguiti tramite una valutazione interna del rischio legato alla compliance, audit che riguardano argomenti specifici di protezione dati e altre verifiche. Il Responsabile della protezione dati del Gruppo ha il diritto di esigere altre verifiche. I risultati devono essere comunicati al Responsabile della protezione dati del Gruppo, alla società del Gruppo responsabile e al suo responsabile della protezione dei dati, qualora sia stato nominato.

Il Consiglio direttivo di Mercedes-Benz Group AG deve essere informato dei risultati nell'ambito degli obblighi di notifica esistenti. Su richiesta, i risultati delle verifiche sono messi a disposizione dell'autorità di controllo per la protezione dati competente. Quest'ultima, nei limiti dei poteri ad essa conferiti dalla legislazione nazionale, può sottoporre ogni società del Gruppo a un audit sulla protezione dati per accertare il rispetto delle disposizioni della presente direttiva.

14 Modifiche alla presente direttiva e collaborazione con le autorità pubbliche

14.1 Responsabilità in caso di modifiche

La presente direttiva può essere modificata in accordo con il Responsabile della protezione dati del Gruppo e nel rispetto della procedura definita per la modifica di direttive (Direttiva sulla gestione di direttive, A 1). Le modifiche che comportano conseguenze significative sulla direttiva sulla protezione dati UE, A 17 stessa o che possono compromettere il livello di protezione offerto (ossia modifiche al carattere vincolante) devono essere prontamente comunicate alle autorità per la protezione dati competenti, le quali emettono l'autorizzazione alla presente direttiva sotto forma di norme vincolanti d'impresa.

Il Responsabile della protezione dati del Gruppo deve tenere un elenco aggiornato di tutte le società del Gruppo vincolate dalla presente direttiva (altra norma applicabile “Elenco delle società del Gruppo vincolate dalla Direttiva sulla protezione dati UE”). Sulla base della presente direttiva, non vengono inoltrati dati personali a una nuova società del Gruppo finché questa non sia vincolata efficacemente alla presente direttiva e non adotti provvedimenti di compliance adeguati al rispetto della direttiva.

L'interessato ha il diritto di accedere facilmente alla presente direttiva. Pertanto la versione più aggiornata della presente direttiva è pubblicata in Internet al sito https://www.group.mercedes-benz.com alla voce relativa alla protezione dati. Questa disposizione è un diritto del terzo beneficiario per l'interessato.

In caso di modifiche alla presente direttiva o all'elenco di società del Gruppo associate, l'autorità di controllo dello stabilimento principale di Mercedes-Benz Group AG ne riceve comunicazione una volta all'anno dal Responsabile della protezione dati del Gruppo, con una breve esposizione delle ragioni dell'aggiornamento.

14.2 Cooperazione con le autorità

Le società del Gruppo che eseguono il trattamento in Paesi terzi o vi partecipano sono obbligate a cooperare con le autorità di controllo responsabili per questioni relative a problemi, indagini o altre procedure connesse al trattamento di dati personali nel contesto summenzionato. È compreso l'obbligo di accettare audit legittimi da parte delle autorità di controllo. Inoltre si devono rispettare tutte le istruzioni legittime impartite dalle autorità di controllo responsabili sulla base di procedure di trattamento in Paesi terzi o disposizioni della presente direttiva.

Le disposizioni di cui al paragrafo 14.2 sulla cooperazione con le autorità sono diritti del terzo beneficiario per l'interessato.

14.3 Monitoraggio e segnalazioni relative a regolamenti di Paesi terzi

I responsabili in società di Paesi terzi devono comunicare immediatamente al Responsabile per la protezione dati del Gruppo se per la loro società sussiste la legittima aspettativa che le leggi o altri regolamenti approvati da un Paese o da un'istituzione diversa dall'UE e dai suoi stati membri presentino i seguenti rischi:

- le leggi o i regolamenti sono tali da impedire alla società del Paese terzo in questione o a un'altra società del Gruppo di adempiere i suoi obblighi previsti dalla presente direttiva durante il trattamento dei dati in Paesi terzi, oppure
- le leggi o i regolamenti possono avere seri effetti negativi sui diritti di cui godono gli interessati sulla base della presente direttiva per il trattamento dei dati in Paesi terzi. Questo rischio sussiste soprattutto qualora l'autorità pubblica locale richieda una trasmissione in modo massiccio, sproporzionato e indiscriminato dei dati personali che superi il limite di ciò che è necessario in una società democratica.

Il Responsabile per la protezione dati del Gruppo deve valutare l'impatto e informare l'autorità per la protezione dei dati competente (qualora presente) se si prevede che la disposizione di legge interferisca in modo significativo con le garanzie offerte dalla presente direttiva. Questa disposizione è un diritto del terzo beneficiario per l'interessato.

Se un'autorità pubblica obbliga una società di un Paese terzo ad astenersi dal notificare all'autorità di controllo per la protezione dati la divulgazione dei dati personali, detta società deve adottare tutte le misure adeguate a limitare il più possibile questo divieto o ad annullarlo, e a fornire annualmente all'autorità di controllo per la protezione dati, entro questo margine di manovra, informazioni generali sulle richieste che ha ricevuto (ad es. numero di richieste di divulgazione, tipo di dati richiesti, identità del richiedente, se possibile).

Mercedes-Benz Group AG, Mercedesstraße 120, 70327 Stuttgart, Germany, www.group.mercedes-benz.com