DAIMLER

Direttiva sulla protezione dati

Premessa

Gentili Signore e Signori,

nell'epoca digitale noi offriamo al cliente la possibilità di essere "sempre connesso" anche in auto, a condizione però che sia possibile procedere al rilevamento e all'elaborazione dei suoi dati. Tuttavia sia a bordo, che durante la manutenzione o l'acquisto di un veicolo, per noi vale sempre la stessa regola: ovunque vengano memorizzati e trasmessi dati, bisogna comunque garantire alti livelli di protezione e di sicurezza. Questo vale tanto per i dati dei clienti, dei possibili acquirenti e dei partner commerciali, quanto per quelli dei nostri collaboratori: perché proteggere i dati significa proteggere le persone.

Il nostro obiettivo è fare in modo che Daimler non sia soltanto sinonimo di auto sicure, ma anche un modello di riferimento per gli standard di protezione dei dati. Per questo motivo, come Gruppo che opera a livello globale, riteniamo che sia un nostro dovere rispettare le diverse normative sulla raccolta ed elaborazione dei dati personali vigenti nei Paesi di tutto il globo. Assicurare uno standard di trattamento dati unificato e valido in ogni parte del mondo per noi è un obiettivo che riveste la massima priorità, anche perché tutelare i diritti di protezione dei dati personali e la sfera privata di ciascun individuo rappresenta la base su cui poter fondare rapporti commerciali improntati alla fiducia.

Nella Corporate Policy Protezione Dati abbiamo stabilito severi requisiti per il trattamento dei dati personali dei clienti, dei possibili acquirenti, dei partner commerciali e dei nostri collaboratori. Questa norma ottempera ai requisiti della Direttiva Europea sulla Protezione dei Dati Personali e garantisce il rispetto dei principi delle leggi sulla privacy nazionali e internazionali riconosciuti in tutto il mondo. Ciò ci consente di applicare a livello aziendale uno standard di protezione e sicurezza dei dati universalmente valido e di disciplinare lo scambio di dati tra le società del nostro Gruppo. Come parametri di riferimento abbiamo stabilito sette principi di trattamento dei dati personali, tra cui figurano trasparenza, economia dei dati e sicurezza dei dati.

I nostri dirigenti e collaboratori hanno l'obbligo di attenersi alla Corporate Policy Protezione Dati e di osservare le leggi sulla privacy in vigore nel rispettivo Paese. Da parte mia, come Responsabile per la Protezione Dati del Gruppo, mi impegno affinché Daimler rispetti le norme di legge e i principi di tutela della privacy in tutto il mondo.

Naturalmente, i miei collaboratori ed io siamo sempre a vostra disposizione per rispondere a qualsiasi quesito sulla protezione e sulla sicurezza dei dati nel Gruppo Daimler.

Dr. Joachim Rieß
Responsabile per la Protezione Dati del Gruppo

Indice

I. Obiettivo della Direttiva sulla protezione dati

Il Gruppo Daimler si impegna, nei limiti della sua responsabilità sociale, al rispetto dei diritti di protezione dei dati personali a livello internazionale. La presente Direttiva sulla protezione dati è valida in tutto il mondo per il Gruppo Daimler e si basa sui principi fondamentali di protezione dati accettati su scala globale. La tutela della protezione dati costituisce la base per la costruzione di rapporti commerciali improntati alla fiducia e per il consolidamento della reputazione del gruppo Daimler come datore di lavoro interessante.

La Direttiva sulla protezione dati crea una delle necessarie condizioni di base per uno scambio globale di dati[1] tra le società del Gruppo. Essa garantisce un livello adeguato di protezione dei dati come richiesto dalla Direttiva Europea sulla Protezione dei Dati Personali[2] e da altre leggi nazionali sullo scambio di dati oltre frontiera, anche nei Paesi in cui fino ad oggi non è stata istituita alcuna legislazione adeguata in materia[3].

II. Ambito di validità e modifica della Direttiva sulla protezione dati

La presente Direttiva sulla protezione dati è valida per tutte le aziende del gruppo Daimler, ovvero per la Daimler AG e tutte le società ad essa dipendenti e collegate, inclusi i rispettivi Collaboratori. “Dipendente” in questo senso significa che la Daimler 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 sulla protezione dati si estende a tutti i processi di elaborazione dei dati personali[4]. Nei Paesi in cui la tutela dei dati delle persone giuridiche è equiparata a quella dei dati personali, la presente Direttiva è valida anche in egual misura per i dati di persone giuridiche. I dati resi anonimi[5], ad es. per valutazioni statistiche o ricerche di mercato, non sono soggetti alla presente Direttiva sulla protezione dati. Le singole società del Gruppo non sono autorizzate a istituire norme in deroga alla presente Direttiva sulla protezione dati. Ulteriori direttive sulla protezione dati possono essere create in accordo con il Responsabile per la Protezione Dati del Gruppo, qualora ciò risulti necessario secondo le norme del rispettivo diritto nazionale. Qualsiasi modifica alla presente Direttiva dovrà essere effettuata esclusivamente in accordo con il Responsabile per la Protezione Dati del Gruppo, nell’ambito della procedura prevista per la modifica delle direttive. Le modifiche dovranno essere comunicate senza indugio alle società del gruppo Daimler secondo quanto prescritto dalla procedura prevista per la modifica delle direttive. Le variazioni che comportano notevoli conseguenze sul rispetto della Direttiva sulla protezione dati devono essere comunicate annualmente alle autorità competenti per la protezione dati preposte all’approvazione della presente Direttiva, in qualità di norme aziendali interne vincolanti sulla protezione dati.

La versione aggiornata della Direttiva sulla protezione dati può essere consultata sotto le avvertenze sulla privacy presenti sul sito Internet della Daimler AG, www.daimler.com.

[1] Vedi cap. XV.

[2] Direttiva 95/46/CE del Parlamento Europeo e del Consiglio Europeo relativa alla tutela delle persone fisiche con riguardo
al trattamento dei dati personali e alla libera circolazione di tali dati;
consultabile all‘indirizzo Internet http://ec.europa.eu/justice_home/fsj/privacy/law/index_de.htm#richtlinie

[3] Vedi cap. XV.

[4] Vedi cap. XV.

[5] Vedi cap. XV.

III. Validità del diritto pubblico

La presente Corporate Policy sulla protezione dati comprende i principi di tutela dei dati personali accettati a livello mondiale, senza sostituirsi al diritto pubblico esistente. Essa integra il rispettivo diritto nazionale vigente in materia di protezione dati. Il diritto pubblico del rispettivo Stato deve prevalere, laddove esso contenga deroghe obbligatorie alla presente Corporate Policy o norme più restrittive. Ai contenuti della presente Corporate Policy è obbligatorio attenersi anche qualora non sussista alcuna norma di diritto pubblico corrispondente. Gli obblighi di dichiarazione derivanti dal diritto pubblico per il trattamento dei dati personali devono essere osservati.

Ogni società del gruppo Daimler è responsabile del rispetto della presente Direttiva sulla protezione dati e dei relativi obblighi di legge. Qualora essa abbia motivo di supporre che gli obblighi di legge siano in contrasto con i doveri derivanti dalla presente Direttiva, la società del Gruppo interessata deve informare immediatamente il Responsabile per la Protezione Dati del Gruppo. In caso di contrasto fra la norma giuridica nazionale e la Direttiva sulla protezione dati, la Daimler AG dovrà ricercare insieme alla società del Gruppo interessata una soluzione fattibile che corrisponda alle finalità della Direttiva stessa.

IV. Principi di trattamento dei dati personali

1. Correttezza e legalità

Nel trattamento dei dati personali bisogna tutelare il diritto alla privacy dell'interessato[6].
I dati personali devono essere trattati in modo legittimo e corretto.

2. Vincolo alle finalità

Il trattamento dei dati personali deve esclusivamente perseguire le finalità stabilite prima del rilevamento dei dati. Eventuali modifiche a posteriori degli scopi del rilevamento sono consentite solo in misura limitata e necessitano di una giustificazione.

3. Trasparenza

L'interessato deve essere informato del trattamento dei suoi dati. Di norma, i dati personali devono essere rilevati presso l'interessato stesso. Durante il rilevamento dei dati, l'interessato deve poter identificare o essere informato su quanto segue:

- l'identità del responsabile del trattamento dati;[7]
- la finalità del trattamento dei dati;
- terzi[8] o categorie di terzi ai quali i dati vengono eventualmente trasmessi.

[6] Vedi cap. XV.
[7] Vedi cap. XV.
[8] Vedi cap. XV.

4. Esclusione ed economia dei dati
Prima del trattamento di dati personali occorre verificare se e in quale misura questi siano necessari per ottenere il fine prefissato con l'elaborazione. Se ciò è possibile per il raggiungimento dell'obiettivo e la mole di lavoro è adeguatamente rapportata al fine prefissato, è preferibile utilizzare dati anonimi o statistici.

I dati personali non possono essere archiviati a titolo di riserva per potenziali finalità future, a meno che ciò non sia previsto o consentito dalle norme di diritto pubblico.

5. Cancellazione
I dati personali non più necessari, dopo la scadenza dei termini di archiviazione previsti dalla legge o dai processi commerciali[9], devono essere cancellati. Qualora, in singoli casi, sussistano motivi per supporre la necessità della tutela di notevoli interessi o la rilevanza storica dei suddetti dati, questi ultimi dovranno rimanere archiviati fino a quando il loro valore non venga stabilito giuridicamente o gli archivi del Gruppo non sia in grado di valutare la necessità di archiviazione dei dati per fini storici.

6. Correttezza oggettiva ed attualità dei dati
I dati personali da archiviare devono essere esatti, completi e inoltre, laddove necessario, costantemente aggiornati. A tale proposito bisogna adottare misure adeguate per assicurare che tutti i dati non corrispondenti, incompleti od obsoleti vengano cancellati, rettificati, integrati o aggiornati.

7. Segretezza e sicurezza dei dati
Per i dati personali vige il vincolo di segretezza. Essi devono essere trattati in modo confidenziale e protetti mediante idonee misure tecniche ed organizzative da accessi non autorizzati, trattamento o diffusione illegale, come pure perdita, modifica o distruzione per errore.

V. Ammissibilità del trattamento dei dati

Il rilevamento, l'elaborazione e l'utilizzo dei dati personali è ammesso esclusivamente quando sussiste una delle seguenti circostanze di fatto giustificative. Tali circostanze di fatto sono necessarie anche nel caso in cui occorra modificare la finalità di rilevamento, elaborazione e utilizzo dei dati personali rispetto alla finalità originaria.

[9] Vedi cap. XV.

1. Dati di Clienti e Partner Commerciali

1.1 Trattamento dati ai fini di un rapporto contrattuale

I dati personali del Soggetto interessato, Cliente o Partner, possono essere elaborati ai fini della costituzione, esecuzione o conclusione di un contratto. Quanto sopra comprende anche l'assistenza fornita al partner contrattuale, qualora ciò sia in relazione ai fini del contratto. Nella fase preliminare di un contratto, ovvero in corso di avviamento del rapporto commerciale, è ammessa l'elaborazione di dati personali per la formulazione di offerte, la preparazione di richieste di acquisto o la soddisfazione di altre richieste dell'interessato orientate alla conclusione dell'accordo. 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. Per ulteriori azioni pubblicitarie occorre attenersi ai requisiti di cui al paragrafo V.1.2.

1.2 Trattamento dati a fini pubblicitari

Qualora l'interessato si rivolga ad un'azienda del gruppo Daimler con una richiesta di informazioni (ad es. per l'invio di materiale informativo su un prodotto), il trattamento dati finalizzato a soddisfare tale richiesta è ammissibile.

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, a condizione che sia compatibile con lo scopo per il quale i dati sono stati originariamente rilevati. L'interessato deve essere informato dell'utilizzo dei suoi dati a fini pubblicitari. Laddove i dati vengano rilevati 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[10] al trattamento dei suoi dati a fini pubblicitari. Nel rilasciare il proprio consenso, l'interessato deve poter scegliere fra diversi canali di contatto disponibili, come ad esempio posta, e-mail e telefono (Consenso, vedi V.1.3).

Nel caso in cui il Soggetto interessato dovesse opporsi 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.

1.3 Consenso al trattamento di dati personali

Il trattamento dei dati personali può avere luogo sulla base del consenso dell'interessato. Prima di rilasciare il consenso, l'interessato deve essere informato ai sensi del paragrafo IV.3 della presente Direttiva sulla protezione dati. Per motivi di documentazione, la dichiarazione di consenso deve essere fornita di norma per iscritto o elettronicamente. In alcuni casi, ad esempio in caso di consulenza telefonica, il consenso può essere fornito anche verbalmente. Il suo rilascio deve comunque essere documentato.

1.4 Trattamento dati sulla base di autorizzazioni legali

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 corrispondenti ai requisiti prescritti dalla legge e commisurati alle relative norme.

[10] Vedi cap. XV.

1.5 Trattamento dati sulla base di interessi giustificati

Il trattamento di dati personali è ammesso anche nel caso in cui ciò sia necessario ai fini della realizzazione di un interesse giustificato del gruppo Daimler. Con interessi giustificati si intendono di norma interessi di carattere legale (ad esempio l'affermazione di diritti) od economico (ad es. la prevenzione di interferenze contrattuali). L'elaborazione dei dati personali sulla base di un interesse giustificato non può avvenire se nel singolo caso esiste il dubbio che gli interessi sensibili del Soggetto interessato prevalgano sull'interesse al trattamento dei dati. Questo aspetto deve essere verificato caso per caso.

1.6 Trattamento di dati sensibili

Il trattamento di dati sensibili[11] è consentito esclusivamente se prescritto dalla legge oppure se l'interessato ha espressamente rilasciato il proprio consenso a tale proposito. Il trattamento di questi dati è ammesso anche qualora risulti necessario per rivendicare, esercitare o difendere diritti legali nei confronti del Soggetto interessato. Laddove si preveda il trattamento di dati sensibili, il Responsabile per la Protezione Dati del Gruppo deve essere informato anticipatamente.

1.7 Decisioni individuali automatizzate

Le elaborazioni automatizzate di dati personali, attraverso cui vengono valutate singole caratteristiche della personalità (ad es. affidabilità creditizia), non possono costituire la base esclusiva di decisioni con conseguenze negative o gravi ripercussioni per il Soggetto interessato. Al Soggetto interessato deve essere comunicata la circostanza e il risultato della decisione individuale automatizzata e la possibilità di una presa di posizione. Per evitare errori decisionali bisogna garantire un controllo e una verifica di plausibilità da parte di un Collaboratore.

1.8 Dati utente e Internet

Se su pagine Web o nelle Apps vengono raccolti, elaborati e utilizzati dati personali, gli interessati devono essere informati al riguardo con apposite avvertenze sulla protezione dati ed eventualmente anche sui cookies. Le avvertenze sulla protezione dati e le eventuali note sui cookies devono essere integrate in modo tale da risultare per gli interessati facilmente riconoscibili, direttamente accessibili e costantemente disponibili.

Qualora per la valutazione del comportamento di utilizzo delle pagine Web e delle Apps vengano utilizzati profili utente (Tracking), gli interessati devono essere in ogni caso informati in proposito nelle avvertenze sulla protezione dati. Il Tracking riferito ad una persona può avere luogo solo se il diritto nazionale lo consente o l'interessato ha rilasciato il proprio consenso. Laddove il Tracking avvenga sotto uno pseudonimo, nelle avvertenze sulla protezione dati bisogna offrire all'interessato la possibilità di rifiuto del consenso (Opt-out).

Qualora le pagine Web o le Apps, in una sezione con obbligo di registrazione, consentano l'accesso a dati personali, il processo di identificazione e autenticazione dell'interessato deve essere configurato in modo tale da garantire una protezione adeguata per il rispettivo accesso.

[11] Vedi cap. XV.

2. Dati dei Collaboratori

2.1 Trattamento dati finalizzato al rapporto lavorativo

Ai fini del rapporto lavorativo è consentito il trattamento dei dati necessari per la stipula, l'esecuzione e la rescissione del contratto di lavoro.
Per consentire l'avviamento di un rapporto di lavoro è possibile elaborare i dati personali dei candidati. Dopo il rifiuto del candidato, i dati di quest'ultimo devono essere cancellati tenendo conto dei termini legali previsti, a meno che il candidato non abbia acconsentito ad un'ulteriore archiviazione per un successivo processo di selezione. 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.

Il trattamento dei dati deve essere sempre riferito alle finalità del contratto di lavoro, a meno che non sussista uno dei successivi 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.

Per il trattamento di dati personali che rientrano nel contesto del rapporto di lavoro, ma non attengono originariamente all'esecuzione del contratto lavorativo, deve sussistere di volta in volta una legittimazione giuridica che può consistere in requisiti di legge, in clausole dei contratti collettivi con le rappresentanze dei lavoratori, nel consenso del Collaboratore o anche negli interessi giustificati dell'azienda.

2.2 Trattamento dati sulla base di autorizzazioni legali

Il trattamento di dati personali 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 conformi ai requisiti prescritti dalla legge e commisurati alle relative norme. Qualora sussista un margine di manovra giuridico, bisogna comunque tutelare gli interessi sensibili del Collaboratore.

2.3 Clausole dei contratti collettivi sul trattamento dati

Se un trattamento dati esula dalle finalità contrattuali, esso è comunque consentito qualora sia ammesso da una clausola dei contratti collettivi. I contratti collettivi sono convenzioni tariffarie o accordi stipulati fra datori di lavoro e rappresentanti dei lavoratori nell'ambito delle possibilità previste dal rispettivo diritto del lavoro. Le clausole devono estendersi allo scopo concreto del trattamento dati richiesto e sono configurabili nell'ambito del diritto nazionale vigente sulla protezione dei dati.

2.4 Consenso al trattamento dei dati personali

Il trattamento dei dati personali dei Collaboratori può avere luogo sulla base del consenso dell'interessato. Le dichiarazioni di consenso devono essere rilasciate spontaneamente. 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. In caso di rilascio spontaneo e informato dei dati da parte dell'interessato è lecito supporre il suo consenso, qualora il diritto nazionale non preveda l'obbligo di un consenso esplicito. Prima di rilasciare il consenso, l'interessato deve essere informato ai sensi del paragrafo IV.3 della presente Direttiva sulla protezione dati.

2.5 Trattamento dati sulla base di interessi giustificati

Il trattamento di dati personali dei Collaboratori è ammesso anche nel caso in cui ciò sia necessario ai fini della realizzazione di un interesse giustificato del gruppo Daimler. Con interessi giustificati si intendono di norma interessi di carattere legale (ad esempio la rivendicazione, l'esercizio o la difesa di diritti giuridici) od economico (ad es. valutazione di aziende).

L'elaborazione dei dati personali sulla base di un interesse giustificato non può avvenire se nel singolo caso esiste il dubbio che gli interessi sensibili del Collaboratore prevalgano sull'interesse al trattamento dei dati. Questo aspetto deve essere verificato caso per caso.

I provvedimenti di controllo che richiedono il trattamento dei dati del Collaboratore possono essere adottati soltanto se esiste un obbligo di legge o un motivo giustificato. Anche in presenza di un motivo giustificato deve comunque essere verificata la proporzionalità della misura di controllo. Gli interessi motivati dell'azienda allo svolgimento della misura 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 dei dati sensibili del Collaboratore interessato dal provvedimento e possono essere imposti soltanto se risultano ragionevoli. L'interesse giustificato dell'azienda 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 di diritto pubblico (ad es. diritti di cogestione della rappresentanza sindacale e diritti all'informazione degli interessati).

2.6 Trattamento di dati sensibili

I dati sensibili possono essere trattati solo a determinate condizioni. Con dati sensibili si intendono le informazioni su origini razziali ed etniche, opinioni politiche, convinzioni religiose o filosofiche, sull'appartenenza ad organizzazioni sindacali o sulla salute o vita sessuale dell'interessato. In base alle norme di diritto pubblico, anche altre categorie di dati possono essere classificate come sensibili oppure il contenuto di queste categorie può essere configurato in modo diverso. Inoltre i dati di carattere giudiziario possono essere trattati solo a particolari condizioni stabilite dalle norme di diritto pubblico.

Il trattamento dei dati deve essere espressamente consentito o prescritto dalla legislazione dello Stato. Inoltre, l'elaborazione è consentita qualora risulti necessaria per permettere al responsabile del trattamento dati di adempiere ai propri diritti e doveri nel campo del diritto del lavoro. Il Collaboratore può anche fornire esplicitamente il proprio consenso al trattamento dei dati.

Laddove si preveda il trattamento di dati sensibili, il Responsabile per la Protezione Dati del Gruppo deve essere informato anticipatamente.

2.7 Decisioni automatizzate

Qualora nel rapporto di lavoro sia prevista l'elaborazione automatizzata di dati personali attraverso i quali vengono valutate singole caratteristiche della personalità (ad es. nell'ambito della selezione del personale o della valutazione di profili di competenze), tale processo automatizzato non può costituire la base esclusiva di decisioni con conseguenze negative o gravi ripercussioni per i Collaboratori interessati. Per evitare errori decisionali nel processo auto matizzato, bisogna garantire che i risultati del processo vengano valutati nei contenuti da una persona fisica e che tale valutazione costituisca la base della decisione da intraprendere. Al Collaboratore interessato deve essere inoltre comunicata la circostanza e il risultato della decisione individuale automatizzata e la possibilità di una presa di posizione.

2.8 Telecomunicazioni e Internet

Apparecchi telefonici, indirizzi e-mail, Intranet e Internet e i social network interni vengono messi a disposizione dall'azienda in primo luogo ai fini dello svolgimento delle mansioni aziendali. Essi rappresentano pertanto strumenti di lavoro e risorse aziendali che possono essere utilizzati nell'ambito delle disposizioni di legge vigenti e delle direttive interne dell'azienda. Qualora le apparecchiature di telecomunicazione siano utilizzabili anche per scopi privati, occorre attenersi all'obbligo di segretezza delle telecomunicazioni e al rispettivo diritto vigente a livello nazionale.

Sulle comunicazioni telefoniche e di posta elettronica, come pure sull'utilizzo delle reti Intranet e Internet, non ha luogo alcun controllo generale. Per evitare attacchi alle infrastrutture IT o a singoli utenti è tuttavia possibile implementare misure di protezione sugli accessi alla rete Daimler, in grado di bloccare contenuti tecnicamente dannosi o analizzare i modelli di eventuali attacchi informatici. Per motivi di sicurezza, l'utilizzo di apparecchi telefonici, indirizzi e-mail, reti Intranet e Internet, nonché dei social network interni, può essere registrato per un determinato periodo di tempo. Le valutazioni di questi dati con riferimenti personali possono avere luogo solo in caso di un sospetto motivato di violazione delle leggi o delle direttive del gruppo Daimler. Questi controlli possono essere eseguiti solo dai settori responsabili delle indagini e nel rispetto del principio di proporzionalità. In tale ambito vanno osservate sia le rispettive leggi nazionali che i regolamenti aziendali vigenti in materia.

VI. Trasmissione di dati personali

Per la trasmissione di dati personali a soggetti esterni al gruppo Daimler o a destinatari interni al gruppo Daimler devono essere soddisfatti i requisiti di ammissibilità dell'elaborazione dei dati personali di cui al paragrafo V. Il destinatario dei dati deve essere vincolato all'utilizzo dei medesimi esclusivamente per gli scopi prestabiliti.

In caso di trasmissione dei dati ad un destinatario esterno al gruppo Daimler che risiede in uno Stato terzo[12], quest'ultimo deve garantire un livello adeguato di protezione dei dati conforme alla presente Policy. Quanto sopra non vale se la trasmissione avviene a seguito di un obbligo di legge. Tale obbligo di legge si può evincere dal diritto del Paese in cui risiede la società del Gruppo che trasmette i dati, oppure qualora il diritto del Paese in cui risiede la società del Gruppo riconosca la finalità della trasmissione dei dati perseguita attraverso l'obbligo di legge di uno Stato terzo.

In caso di trasmissione dei dati da parte di terzi ad aziende del gruppo Daimler bisogna assicurare che i dati possano essere utilizzati per le finalità di trattamento previste.

Se i dati personali vengono trasmessi da una società del Gruppo con sede nello Spazio Economico Europeo (SEE) ad una società del gruppo con sede al di fuori del SEE[13] (Stato terzo), la società importatrice dei dati ha l'obbligo, per tutte le richieste delle autorità di controllo competenti per l'organizzazione esportatrice dei dati, di cooperare con esse e di attenersi alle considerazioni delle autorità di controllo in merito ai dati trasmessi. Quanto sopra vale anche per le trasmissioni di dati da parte di società del Gruppo con sedi in altri Stati. Laddove tali società aderiscano ad un sistema di certificazione internazionale per le norme aziendali vincolanti sulla protezione dati, esse devono inoltre garantire la cooperazione prevista in tale ambito con gli organi di controllo e le autorità corrispondenti. L'adesione ai suddetti sistemi di certificazione deve essere concordata con il Responsabile Protezione Dati del Gruppo.

[12] Vedi cap. XV.

[13] Vedi cap. XV.

In caso di una violazione presunta da un Soggetto interessato contro la presente Direttiva sulla protezione dati da parte di una società del Gruppo importatrice di dati con sede in uno Stato terzo, l'azienda del Gruppo esportatrice dei dati con sede nello Spazio Economico Europeo (SEE) si impegna sia a sostenere nel chiarimento della fattispecie il Soggetto interessato, i cui dati sono stati rilevati in ambito SEE, sia ad assicurare l'affermazione dei suoi diritti ai sensi la presente Direttiva sulla protezione dati nei confronti della società del Gruppo importatrice dei dati. Inoltre, il Soggetto interessato ha la facoltà di rivendicare i propri diritti anche nei confronti della società del Gruppo esportatrice dei dati. In caso di presunta violazione, la società esportatrice dei dati deve produrre nei confronti dell'interessato la prova che alla società del Gruppo importatrice dei dati in uno Stato terzo non è imputabile alcuna violazione contro la presente Direttiva sulla protezione dati nel corso del trattamento dei dati ricevuti.

In caso di trasmissione di dati personali da una società del Gruppo con sede nello Spazio Economico Europeo (SEE) ad una società del Gruppo con sede in uno Stato terzo, l'organizzazione che trasmette i dati deve assumersi la propria responsabilità giuridica nei confronti del Soggetto interessato, i cui dati personali sono stati rilevati in ambito SEE, per eventuali violazioni della società del Gruppo con sede in uno Stato terzo contro la presente Direttiva, come se la stessa organizzazione fornitrice dei dati avesse compiuto tale violazione. Il foro competente per quanto sopra è il tribunale preposto alla sede dell'organizzazione esportatrice dei dati.

VII. Trattamento dati per conto terzi

Il trattamento dati per conto terzi ha luogo quando un Fornitore esterno viene incaricato dell'elaborazione dati, senza tuttavia alcun trasferimento di responsabilità per il relativo processo aziendale. In questi casi è necessario stipulare un accordo sul trattamento dei dati sia con i fornitori esterni che tra le aziende del gruppo Daimler. In tale ambito, il Committente si assume la piena responsabilità per la correttezza del processo di trattamento dati. Il Fornitore può elaborare i dati personali solo entro i limiti delle direttive ricevute dal Committente. Inoltre, al conferimento dell'incarico si devono osservare le regole elencate qui di seguito, la cui attuazione deve essere assicurata dal reparto tecnico competente.

1. Il Fornitore deve essere selezionato in base alla sua idoneità a garantire le necessarie misure di sicurezza tecniche e organizzative.
2. L'incarico deve essere conferito per iscritto. Nel conferimento devono essere documentate sia le istruzioni per il trattamento dei dati che le responsabilità del Committente e del Fornitore.
3. Il rispetto degli standard contrattuali stabiliti dal Responsabile Protezione Dati del Gruppo è obbligatorio.
4. Prima di iniziare il trattamento dei dati, il Committente deve essere convinto dell'idoneità del Fornitore a rispettare i doveri prescritti. In particolare, il rispetto dei requisiti di sicurezza dei dati può essere dimostrato dal Fornitore presentando un'idonea certificazione. A seconda del livello di rischio del processo di elaborazione dei dati, è possibile eventualmente ricorrere a regolari controlli periodici dell'osservanza dei suddetti criteri durante il periodo contrattuale.

5. Nel caso di affidamento dell'incarico di trattamento dati a fornitori oltre frontiera occorre rispettare i corrispondenti requisiti nazionali per la trasmissione di dati personali all'estero. In particolare, l'elaborazione di dati personali provenienti dallo Spazio Economico Europeo in uno Stato terzo può avere luogo solo se il Fornitore dimostra di possedere un livello di protezione dei dati equiparabile ai requisiti della presente Direttiva. A tale scopo possono risultare idonei i seguenti strumenti:
   a. accordo sulle clausole contrattuali standard dell'UE per il trattamento dati per conto terzi in Stati terzi con il Fornitore ed eventuali subappaltatori;
   b. adesione del Fornitore ad un sistema di certificazione riconosciuto dall'UE per la creazione di un livello di protezione dati adeguato;
   c. riconoscimento di regole aziendali vincolanti del Fornitore per la creazione di un livello di protezione dati adeguato da parte delle autorità competenti in materia di privacy.

VIII. Diritti del Soggetto interessato

Ogni Soggetto interessato può far valere i seguenti diritti, la cui rivendicazione deve essere affidata senza indugio al settore responsabile e non deve comportare alcuna ripercussione negativa per l'interessato.

1. Il Soggetto interessato può esigere informazioni su quali dei suoi dati personali, e con quale provenienza e a quale scopo, siano stati archiviati. Qualora, secondo il rispettivo diritto del lavoro vigente, sussistano ulteriori diritti alla visione dei documenti del datore di lavoro (ad es. documenti del personale), questi ultimi rimangono inalterati.
2. Nel caso in cui i dati personali vengano trasmessi a terzi, devono essere fornite informazioni sull'identità del destinatario o sulle categorie di destinatari.
3. Nel caso in cui i dati personali dovessero risultare inesatti o incompleti, il Soggetto interessato può richiederne la correzione o integrazione.
4. Il Soggetto interessato può opporsi al trattamento dei suoi dati personali a fini di pubblicità diretta o ricerche di mercato e di opinione. Pertanto, i relativi dati devono essere resi inaccessibili a tali finalità.
5. Il Soggetto interessato è autorizzato a richiedere la cancellazione dei suoi dati se le basi giuridiche per l'elaborazione dei dati risultano assenti o non più valide. Lo stesso vale nel caso in cui lo scopo dell'elaborazione dei dati sia decaduto a causa della decorrenza dei termini prescritti o per altri motivi. Gli obblighi di archiviazione esistenti e gli interessi sensibili contrari alla cancellazione di dati devono comunque essere rispettati.
6. Il Soggetto interessato possiede in generale il diritto di opporsi all'elaborazione dei propri dati che deve essere preso in considerazione qualora il suo interesse sensibile, a causa di una particolare situazione personale, prevalga sull'interesse al trattamento dei dati. Quanto sopra non vale se una norma di legge obbliga in ogni caso a procedere all'elaborazione dei dati.

Inoltre ogni Soggetto interessato può far valere i diritti menzionati ai punti III. par. 2, IV., V., VI., IX., X, e XIV. par. 3 come terzo beneficiario, qualora un'azienda che si è impegnata al rispetto della Direttiva sulla protezione dati, non rispetti le relative disposizioni e in tal modo leda i diritti dell'interessato stesso.

IX. Segretezza del trattamento dati

I dati personali sono soggetti all'obbligo di segretezza. I Collaboratori non possono rilevare, elaborare o utilizzare dati personali senza autorizzazione. Come non autorizzato si intende qualsiasi trattamento dei dati che un Collaboratore effettua senza essere incaricato e abilitato a tale scopo nell'ambito dell'esercizio delle sue funzioni. A tale proposito si applica il principio del "need to know": i Collaboratori possono avere accesso a dati personali solo quando necessario e nella misura richiesta per lo svolgimento delle rispettive mansioni. Quanto sopra richiede un'attenta suddivisione e separazione di ruoli e competenze, nonché la relativa implementazione e cura nell'ambito dei processi di autorizzazione.

I Collaboratori non possono utilizzare dati personali per scopi privati o economici, trasmetterli a persone non autorizzate e renderli accessibili a terzi in altro modo. I Dirigenti devono informare i rispettivi Collaboratori sugli obblighi di mantenimento della segretezza dei dati fin dall'inizio del rapporto lavorativo. Questo obbligo sussiste anche dopo la conclusione del rapporto di lavoro.

X. Sicurezza del trattamento dati

I dati personali devono essere sempre protetti da accessi non autorizzati, trattamento o diffusione illegale, come pure perdita, modifica o distruzione per errore. Quanto sopra vale indipendentemente dalla modalità di trattamento dei dati, sia esso elettronico che in forma cartacea. Prima dell'introduzione di nuovi processi di elaborazione dati, e in particolare di nuovi sistemi informatici, occorre stabilire e implementare idonee misure tecniche e organizzative per la protezione dei dati personali. Queste misure devono essere all'avanguardia della tecnica e tenere conto dei rischi derivanti dal trattamento dei dati, come pure del fabbisogno di protezione dei medesimi (rilevato attraverso il processo di classificazione delle informazioni). Il reparto tecnico competente può rivolgersi per una consulenza in particolare al rispettivo Responsabile Sicurezza Informazioni (ISO) e al Coordinatore Protezione Dati. Queste misure tecniche e organizzative per la protezione dei dati personali fanno parte di un sistema integrato di sicurezza nella gestione delle informazioni a livello di tutto il Gruppo e devono essere continuamente adeguate agli sviluppi tecnici e alle modifiche organizzative.

XI. Controllo sulla protezione dati

L'osservanza delle direttive sulla protezione dati e delle corrispondenti leggi in vigore viene verificata attraverso regolari processi di auditing e ulteriori controlli. L'esecuzione dei controlli spetta al Responsabile Protezione Dati del Gruppo, ai Coordinatori della Protezione Dati e ad ulteriori settori aziendali con diritti di auditing o revisori esterni incaricati. I risultati dei controlli sulla protezione dati devono essere comunicati al Responsabile Protezione Dati del Gruppo.
Il Consiglio di Vigilanza della Daimler AG deve essere informato di eventuali risultati di rilievo, nell'ambito dei rispettivi obblighi di rendicontazione. Su richiesta, i risultati dei controlli sulla protezione dati devono essere messi a disposizione delle autorità competenti in materia di tutela della privacy. Le autorità competenti, nei limiti dei poteri ad esse conferiti dalle norme di diritto pubblico, possono anche eseguire propri controlli sul rispetto delle disposizioni della presente Direttiva.

XII. Violazioni della privacy

Ogni Collaboratore deve segnalare senza indugio al rispettivo superiore, al proprio Coordinatore della Protezione Dati o al Responsabile Protezione Dati del Gruppo, i casi di presunta violazione contro la presente Direttiva o altre norme sulla protezione dei dati personali (violazioni della privacy[14]). Il Dirigente responsabile della funzione o dell'unità interessata ha l'obbligo di informare immediatamente dei suddetti casi il Coordinatore della Protezione Dati competente o il Responsabile Protezione Dati del Gruppo.

Nei casi di
- illecita trasmissione di dati personali a terzi,
- accesso non autorizzato a dati personali da parte di terzi, oppure
- perdita di dati personali

occorre procedere senza indugio alle segnalazioni previste in azienda (Information Security Incident Management), allo scopo di ottemperare agli obblighi di denuncia delle violazioni della privacy previsti dalle norme di diritto pubblico.

XIII. Responsabilità e sanzioni

I Consigli di Amministrazione e i Dirigenti delle società del Gruppo, in qualità di responsabili del trattamento dati nella rispettiva sfera di competenza, hanno l'obbligo di assicurare l'osservanza dei requisiti di legge e dei criteri formulati nelle direttive sulla protezione dei dati (ad es. obbligo di denuncia alle autorità nazionali). Nei compiti manageriali dei Dirigenti rientra quello di garantire attraverso misure organizzative, personali e tecniche, un trattamento dati regolare nel rispetto della privacy. L'attuazione delle suddette misure rientra nelle responsabilità dei Collaboratori competenti. In caso di controlli sulla protezione dati da parte delle autorità competenti, il Responsabile Protezione Dati del Gruppo deve essere informato senza indugio.

Le rispettive direzioni aziendali e di fabbrica devono nominare un Coordinatore da affiancare al Responsabile Protezione Dati. A livello organizzativo, in accordo con il Responsabile Protezione Dati del Gruppo, questo ruolo può anche essere assunto da un Coordinatore competente per diverse società o fabbriche. Questi Coordinatori, che rappresentano i referenti per la protezione dati a livello locale, possono eseguire controlli e devono rendere noti ai Collaboratori i contenuti delle direttive sulla protezione dati. Le rispettive direzioni aziendali hanno l'obbligo di assistere il Responsabile Protezione Dati del Gruppo e i relativi Coordinatori nello svolgimento delle loro attività.

I responsabili tecnici di processi e progetti aziendali devono informare tempestivamente i Coordinatori della protezione dati di eventuali nuove elaborazioni di dati personali. In caso di progetti di elaborazione dati che possono comportare particolari rischi per la tutela della privacy degli interessati, il Responsabile Protezione Dati del Gruppo deve essere coinvolto già da prima dell'inizio del processo di trattamento delle informazioni. Quanto sopra vale in particolare per i dati personali sensibili. I Dirigenti devono provvedere affinché i loro Collaboratori vengano istruiti nella misura necessaria alla protezione dei dati personali.

Eventuali abusi nell'elaborazione dei dati personali o altre violazioni contro il diritto alla protezione dei dati vengono perseguiti in molti Stati anche penalmente e possono comportare richieste di risarcimento di danni. Inoltre, le infrazioni per le quali possono essere ritenuti responsabili singoli Collaboratori possono dare luogo a sanzioni disciplinari.

[14] Vedi cap. XV.

XIV. Il Responsabile Protezione Dati del Gruppo

Il Responsabile Protezione Dati del Gruppo, come organo interno tecnicamente indipendente, vigila sul rispetto delle norme nazionali ed internazionali di protezione dei dati. Egli è responsabile per le direttive sulla protezione dati e ne controlla l'osservanza. Il Responsabile Protezione Dati del Gruppo viene nominato dal Consiglio Direttivo della Daimler AG. Anche le società del Gruppo con obbligo di nomina designano generalmente il responsabile del Gruppo come responsabile legale della protezione dei dati. Eventuali eccezioni devono essere concordate con il Responsabile Protezione Dati del Gruppo.

I Coordinatori della Protezione Dati hanno l'obbligo di comunicare tempestivamente al Responsabile Protezione Dati del Gruppo eventuali rischi per la sicurezza dei dati.

Qualunque Soggetto interessato può rivolgersi in qualsiasi momento al Responsabile Protezione Dati del Gruppo o al rispettivo Coordinatore competente per suggerimenti, richieste, domande di informazioni o reclami relativi al tema della protezione dati. Se lo si desidera, tali richieste e reclami potranno essere trattati come confidenziali.

Qualora il Coordinatore competente non possa risolvere un reclamo oppure porre rimedio a una violazione contro le direttive sulla protezione dei dati, egli deve contattare il Responsabile Protezione Dati del Gruppo. Le decisioni di quest'ultimo volte a porre rimedio alla violazione devono essere osservate dalle rispettive direzioni aziendali. Le richieste delle autorità di vigilanza sulla privacy devono essere sempre portate a conoscenza anche del Responsabile Protezione Dati del Gruppo.

Il Responsabile Protezione Dati del Gruppo e i suoi Collaboratori possono essere contattati ai seguenti recapiti:
Daimler AG, Responsabile Protezione Dati del Gruppo,
HPC 0518, D-70546 Stoccarda
e-mail: mbox_datenschutz@daimler.com
In Intranet sotto http://intra.corpintra.net/cdp

XV. Definizioni

» Un livello adeguato di protezione dei dati da parte di Paesi terzi viene riconosciuto dalla Commissione dell'Unione Europea quando la sfera privata delle persone, così come viene intesa di comune accordo dagli Stati Membri dell'UE, risulta fondamentalmente protetta. La Commissione UE tiene conto nella sua decisione di tutte le circostanze che svolgono un ruolo nella trasmissione di dati o in una categoria di trasmissioni di dati. Quanto sopra include anche la valutazione delle norme di diritto pubblico, come pure delle rispettive disposizioni del Codice Civile e sulla sicurezza.

» I dati si ritengono anonimi quando non è più possibile stabilire un riferimento personale in modo duraturo e da parte di chiunque, oppure laddove il riferimento personale sia riconducibile solo con un dispendio sproporzionatamente elevato di tempo, costi e mole di lavoro.

- I dati sensibili sono informazioni su origini razziali ed etniche, opinioni politiche, convinzioni religiose o filosofiche, sull'appartenenza ad organizzazioni sindacali o sulla salute o vita sessuale dell'interessato. In base alle norme di diritto pubblico, anche altre categorie di dati possono essere classificate come sensibili oppure il contenuto di queste categorie può essere configurato in modo diverso. Analogamente, i dati di carattere giudiziario possono essere trattati solo a particolari condizioni stabilite dalle norme di diritto pubblico.
- Con soggetto interessato ai sensi della presente Direttiva si intende ogni persona fisica sulla quale vengono elaborati i dati. In alcuni Paesi, i soggetti interessati possono essere anche persone giuridiche.
- Le violazioni della privacy sono tutte le circostanze in cui esiste il fondato sospetto che i dati personali siano stati illecitamente spiati, rilevati, modificati, copiati, trasmessi o utilizzati. Si può riferire sia ad azioni compiute da terzi che ad atti commessi da Collaboratori.
- Con terzi si intende chiunque, escluso l'interessato e il responsabile del trattamento dati. All'interno dell'UE non sono da ritenersi terzi ai sensi del diritto sulla privacy neanche gli addetti all'elaborazione dei dati legalmente subordinati al responsabile del trattamento dati.
- Con Paesi terzi ai sensi della presente Direttiva si intendono tutti gli Stati al di fuori dell'Unione Europea/SEE. Sono esclusi gli Stati con un livello di protezione dei dati riconosciuto come adeguato dalla Commissione UE.
- Il consenso è una dichiarazione di accettazione volontaria e giuridicamente vincolante all'elaborazione dei dati personali.
- Il trattamento di dati personali si ritiene necessario laddove un fine consentito dalla legge o un interesse giustificato non sia raggiungibile, o risulti tale solo con un dispendio sproporzionatamente elevato, senza poter disporre dei relativi dati personali.
- Lo Spazio Economico Europeo (SEE) è un'area economica associata all'Unione Europea a cui appartengono anche la Norvegia, l'Islanda e il Liechtenstein.
- I dati personali sono tutte le informazioni su una determinata o determinabile persona fisica. Una persona si intende determinabile, ad esempio, quando il riferimento personale può essere stabilito attraverso una combinazione di informazioni con una serie di dati supplementari disponibili anche solo casualmente.
- Con trasmissione si intende qualsiasi divulgazione di dati personali protetti da parte del responsabile del trattamento dati a terzi.
- Il trattamento di dati personali è qualsiasi processo eseguito con o senza l'ausilio di processi automatizzati ai fini di rilevamento, memorizzazione, organizzazione, archiviazione, modifica, interrogazione, utilizzo, riproduzione, trasmissione, diffusione o combinazione e confronto di dati. Quanto sopra include anche lo smaltimento, la cancellazione e il blocco di dati e supporti dati.
- Con responsabile del trattamento dati si intende la società giuridicamente indipendente del gruppo Daimler la cui attività aziendale richiede la rispettiva misura di trattamento dei dati.

Daimler AG
Mercedesstraße 137
70327 Stuttgart
Germany
www.daimler.com