Directive sur la protection des données UE

Mercedes-Benz

Sommaire

1 Objectif de la directive

Mercedes-Benz Group considère que le respect des droits en matière de protection des données fait partie de sa responsabilité sociale.

Dans certains pays et régions tels que l'Union européenne, les législateurs ont défini des standards pour la protection des données des personnes physiques (« données à caractère personnel »), incluant l'obligation de ne transférer ces données dans d'autres pays que si la loi locale en vigueur à destination garantit un niveau de protection des données adéquat.

La présente directive sur la protection des données UE établit des standards uniformes et adaptés au sein du Groupe - tant pour :

- (a) le traitement des données à caractère personnel dans des régions telles que l'UE/l'Espace Economique Européen (EEE) (dénommées ci-après uniformément « UE/ EEE ») que pour
- (b) le transfert transfrontalier de données à caractère personnel à des sociétés du Groupe hors de l'UE/EEE (y compris leur traitement consécutif sur place).

La présente directive édicte à cette fin des règles contraignantes pour le traitement des données à caractère personnel issues de l'UE/EEE au sein de Mercedes-Benz Group. Celles-ci fournissent des garanties adéquates en matière de protection des données à caractère personnel hors de l'UE/ EEE et constituent ainsi des règles d'entreprise contraignantes (« Binding Corporate Rules – BCR ») pour Mercedes-Benz Group.

2 Champ d’application

La présente directive sur la protection des données UE s'applique à Mercedes-Benz Group AG, aux sociétés du Groupe qu'il contrôle (ci-après dénommées sociétés du Groupe) ainsi qu'à leurs collaborateurs et aux membres de leurs organes de direction.On entend par « contrôle » le fait que Mercedes-Benz Group AG est en droit d’exiger, de manière directe ou indirecte, l’application de la présente directive, que ce soit sur la base d’une majorité des droits de vote, d’une majorité au sein de la direction de l’entreprise ou d’un accord.

La directive s'applique au traitement entièrement ou partiellement automatisé des données à caractère personnel, ainsi qu'au traitement manuel dans les systèmes de classement sauf si les lois nationales prévoient un champ plus large. En Allemagne, la directive s'applique aussi à toutes les données des collaborateurs[1] au format papier.
La directive s'applique au traitement des données à caractère personnel :

- (a) de sociétés du Groupe et de leurs succursales établies dans l'UE/ EEE ou d'un autre pays auquel cette directive peut être étendue (« sociétés basées dans l'UE/ EEE »),
- (b) de sociétés du Groupe établies hors de l'UE/ EEE si celles-ci proposent des biens ou des services à des personnes physiques au sein de l'UE/ EEE et/ ou elles analysent le comportement de personnes physiques au sein de l'UE/ EEE (« sociétés de pays tiers proposant des offres pour l'UE/ EEE ») ou
- (c) de sociétés du Groupe établies hors de l'UE/ EEE si celles-ci ont reçu directement ou indirectement des données à caractère personnel de sociétés auxquelles la directive s'applique au titre du point a) ou b) ou si lesdites données leur ont été communiquées (« sociétés de pays tiers qui reçoivent des données de l'UE/ EEE »).

[1] Afin de simplifier la lecture du document, seule la forme masculine sera utilisée dans la présente directive pour désigner les personnes physiques. Sur le fond, les contenus concerneront toujours les deux sexes.

Les traitements hors de l'UE/ EEE seront présentés dans la présente directive comme des traitements dans un pays tiers.

Les sociétés du Groupe qui participent à, ou sont soumises à un traitement par des sociétés de pays tiers sont énumérées dans l'autre règlement applicable « Liste des sociétés UE relevant de la directive sur la protection des données UE ».

La présente directive peut être étendue aux pays hors de l'UE/ EEE. Dans les pays où les données des personnes morales sont protégées de la même manière que les données à caractère personnel, la présente directive s'appliquera aussi aux données des personnes morales.

3 Contrainte juridique au sein de Mercedes-Benz Group

Les règles et les dispositions de la présente directive présentent un caractère contraignant pour toutes les sociétés du Groupe opérant dans son champ d'application. Les sociétés du Groupe, de même que leurs dirigeants et leurs collaborateurs, sont donc responsables du respect de la présente directive au même titre que de la conformité à la législation UE applicable et aux lois nationales sur la protection des données en vigueur.

Sauf dispositions légales contraires, les sociétés du Groupe ne sont pas autorisées à adopter des règlements qui divergent de la présente directive.

4 Conformité aux exigences légales

La présente directive ne remplace pas la législation UE et les lois nationales. Elle vient en complément des lois nationales sur la protection des données. Ces règlements et lois s'appliqueront prioritairement si la conformité à cette directive implique une violation de la loi nationale en vigueur. Le contenu de la présente directive doit être respecté en l'absence de lois nationales correspondantes.

Si la conformité à cette directive implique une violation de la loi nationale, ou si des règlements divergeant de cette directive sont requis par la loi nationale, il conviendra d'en informer le délégué à la protection des données du Groupe et l'organisation centrale de la compliance aux fins de contrôle du respect de la loi sur la protection des données. En cas de conflit entre les lois nationales et la présente directive, le délégué à la protection des données du Groupe et l'organisation centrale de la compliance collaboreront avec la société du Groupe responsable pour trouver une solution pratique conforme à la finalité de la présente directive.

5 Principes généraux relatifs au traitement des données à caractère personnel

5.1 Légalité

Les données à caractère personnel doivent être traitées de manière légale et de bonne foi. Le traitement des données ne pourra avoir lieu que si l'activité de traitement se fonde sur une base légale suffisante. Cette disposition s'applique aussi au traitement des données entre les sociétés du Groupe. Le simple fait que les deux sociétés du Groupe, les entreprises de transfert et de réception, soient affiliées à Mercedes-Benz Group ne constitue pas en soi une telle base légale.

Le traitement des données à caractère personnel est légal si l'une des conditions suivantes d'autorisation aux termes des sections 5.2 ou 5.3 s'applique.Ces conditions d'autorisation sont également requises si la finalité du traitement des données à caractère personnel doit être modifiée par rapport à la finalité d'origine.

5.2 Base légale relative aux données client et partenaire

5.2.1 Traitement des données pour une relation contractuelle

Les données à caractère personnel des prospects, clients ou partenaires peuvent être traitées pour établir, exécuter et mettre fin à un contrat. Cette disposition inclut les prestations de conseil destinées au client ou au partenaire sous contrat si celles-ci sont en rapport avec la finalité contractuelle.

Lors de la négociation d'un contrat, les données à caractère personnel peuvent être traitées pour établir des offres, préparer des demandes d'achat ou répondre à d'autres souhaits des prospects en rapport avec la conclusion du contrat. Les prospects peuvent être contactés durant la phase d'initialisation du contrat par le biais des informations qu'ils ont communiquées. Les restrictions éventuelles formulées par le prospect doivent être respectées.

5.2.2 Traitement des données à des fins publicitaires

Si la personne concernée contacte une société du Groupe en demandant plus d'informations (par ex. en demandant de recevoir des informations sur un produit), le traitement des données en vue de répondre à cette demande sera autorisé. Les mesures de fidélisation de la clientèle ou actions publicitaires sont soumises à des conditions légales supplémentaires. Le traitement de données à caractère personnel à des fins de publicité, d'étude de marché ou de sondage d'opinion est autorisé dans la mesure où ce traitement est compatible avec la finalité pour laquelle les données ont été initialement collectées. La personne concernée doit être informée à l'avance de l'utilisation de ses données personnelles à des fins publicitaires. Si les données personnelles ne sont collectées qu'à des fins publicitaires, la personne concernée pourra choisir de fournir ou non ces données. Elle devra être informée du fait que la fourniture de données dans ce contexte s'effectuera sur une base volontaire. Le consentement de la personne concernée devra être obtenu dans le cadre du processus de communication. En accordant son consentement, la personne concernée doit avoir le choix entre différentes formes de prise de contact telles que par e-mail et par téléphone (voir Section 5.2.3 sur le consentement). Si la personne concernée s'oppose à l'utilisation de ses données à des fins publicitaires, celles-ci ne pourront plus être utilisées à cette fin et leur usage dans cette perspective devra être restreint ou bloqué. Il conviendra de respecter toute autre restriction requise par certains pays spécifiques concernant l'utilisation de données à des fins publicitaires.

5.2.3 Consentement au traitement des données

Les données à caractère personnel pourront être traitées après obtention du consentement de la personne concernée. Avant d'accorder son consentement, la personne concernée doit être informée conformément à la présente directive sur la protection des données UE. La déclaration de consentement doit être systématiquement établie sous forme écrite ou électronique afin de pouvoir être utilisée pour les nécessités de la preuve. Dans certaines circonstances, notamment dans le cadre d'une prestation de conseil téléphonique, le consentement peut également être accordé par oral. L'attribution du consentement doit être documentée.

5.2.4 Traitement des données conformément à une autorisation ou une obligation légale

Le traitement de données à caractère personnel est également licite dans les cas où celui-ci est exigé, posé comme condition ou admis du fait de dispositions légales nationales. Le type et l'étendue du traitement des données doivent être nécessaires à l'activité de traitement des données légalement autorisée et conformes aux dispositions légales concernées.

5.2.5 Traitement des données conformément à l'intérêt légitime

Les données à caractère personnel peuvent aussi être traitées si nécessaire pour répondre à un intérêt légitime. Les intérêts légitimes sont généralement de nature légale (par ex. recouvrer des créances en souffrance) ou commerciale (par ex. éviter des violations de contrat). Le traitement ne peut pas s'effectuer sur la base d'un intérêt légitime si, dans une situation spécifique, les intérêts de la personne concernée à protéger l'emportent sur l'intérêt légitime du traitement. Avant tout traitement, il convient de vérifier s'il existe des intérêts sensibles.

5.3 Base légale relative aux données collaborateurs

5.3.1 Traitement des données relatif à la relation de travail

Le traitement des données à caractère personnel nécessaires à l'établissement, à l'exécution ou à la cessation du contrat de travail est autorisé dans le cadre de la relation de travail. Les données à caractère personnel des candidats peuvent être traitées pour aider à la décision d'engager une relation de travail. Si le candidat n'est pas retenu, ses données devront être supprimées dans le respect de la période de conservation requise sauf si le candidat accepte que ses données soient conservées pour un futur processus de sélection. Le consentement du candidat est également nécessaire pour permettre le recours aux données dans le cadre d'autres procédures de recrutement ou préalablement à leur communication à d'autres sociétés du Groupe. Dans la relation de travail existante, le traitement des données doit toujours être en rapport avec la finalité de la relation de travail si aucune des conditions suivantes n'est remplie pour un traitement autorisé des données.

Si, dans la phase initiale de la relation de travail ou au cours de celle-ci, un complément d'information sur le candidat doit être obtenu auprès d'un tiers, il convient alors d'observer les dispositions légales nationales applicables. En cas de doute – si autorisé, le consentement doit être obtenu de la personne concernée.

Une base légale telle que définie ci-dessous doit être établie pour pouvoir traiter les données à caractère personnel en rapport avec la relation de travail, mais ne fait pas initialement partie de la création, de l'exécution ou de la résiliation de la relation de travail (données des collaborateurs).

5.3.2 Traitement des données conformément à une autorisation ou une obligation légale

Le traitement de données des collaborateurs est également licite dans les cas où celui-ci est exigé, posé comme condition ou admis du fait de dispositions légales nationales. Le type et l'étendue du traitement des données doivent être nécessaires à l'activité de traitement des données légalement autorisée et conformes aux dispositions légales concernées. En présence d'une marge de manœuvre légale, les intérêts sensibles du collaborateur doivent être pris en considération.

5.3.3 Convention collective relative au traitement des données

Si une activité de traitement des données va au-delà de la finalité d'exécution d'un contrat, celle-ci pourra rester légale si elle est autorisée par une convention collective. Les accords doivent couvrir la finalité spécifique de l'activité de traitement des données envisagée et être établis dans le respect des paramètres de la législation UE et nationale.

5.3.4 Consentement au traitement des données

Les données des collaborateurs peuvent être traitées avec le consentement de la personne concernée. Les déclarations de consentement doivent être soumises sur une base volontaire. Aucune sanction ne peut être imposée en cas de refus de consentement. Tout consentement donné sur une base non volontaire est réputé sans effet. La déclaration de consentement doit être systématiquement établie sous forme écrite ou électronique afin de pouvoir être utilisée pour les nécessités de la preuve. Si, à titre exceptionnel, les circonstances ne le permettent pas, le consentement peut être accordé par oral. Son attribution devra être dans tous les cas dûment documentée. Avant d'accorder son consentement, la personne concernée doit être informée conformément à la présente directive sur la protection des données UE.

5.3.5 Traitement des données conformément à l'intérêt légitime

Les données des collaborateurs peuvent aussi être traitées si nécessaire pour répondre à un intérêt légitime de la société du Groupe. Les intérêts légitimes sont généralement de nature légale (par ex. constatation, exercice ou défense de droits en justice) ou commerciale (par ex. accélération de processus commerciaux, évaluation de sociétés). Avant le traitement des données, il convient de déterminer s'il existe des intérêts dignes de protection. Les données à caractère personnel peuvent être traitées sur la base d'un intérêt légitime si les intérêts dignes de protection du collaborateur ne l'emportent pas sur l'intérêt du traitement.

Les mesures de contrôle qui requièrent le traitement des données des collaborateurs au-delà de l'exécution de la relation de travail (par ex. contrôles de performances) ne peuvent être mises en œuvre sauf s'il existe une obligation légale ou une raison dûment justifiée à le faire. Même s'il existe une raison légitime, la proportionnalité de la mesure de contrôle doit également être vérifiée. A cette fin, les intérêts légitimes de la société du Groupe à mettre en œuvre la mesure de contrôle (par ex. respect de dispositions légales et de règles internes à l'entreprise) doivent être mis en balance avec tout intérêt protecteur que le collaborateur affecté par la mesure pourrait avoir à exclure la mesure. Les mesures ne devront être prises que si elles sont appropriées dans le cas spécifique. L'intérêt légitime de la société du Groupe et les éventuels intérêts sensibles des collaborateurs doivent être déterminés et documentés avant toute mesure. Par ailleurs, il convient, le cas échéant, de prendre en considération les exigences complémentaires découlant de la législation en vigueur (droits de cogestion des organes de représentation des salariés, droits à l'information des intéressés, par exemple).

5.4 Traitement de données particulièrement sensibles

Le traitement de données à caractère personnel particulièrement sensibles doit être expressément autorisé ou prescrit par la loi nationale. Le traitement de telles données par la société du Groupe peut être autorisé en particulier si la personne concernée a accordé son consentement exprès, si le traitement est nécessaire pour constater, faire valoir ou défendre des droits en justice à l'encontre de la personne concernée ou si le traitement permet au responsable du traitement d'exercer ses droits et responsabilités au regard du droit du travail et du droit social.

Si un traitement des données particulièrement sensibles est programmé, le délégué à la protection des données du Groupe devra en être informé.

5.5 Prise de décision individuelle automatisée (avec éventuellement profilage)

Les personnes concernées peuvent faire l'objet d'une prise de décision entièrement automatisée qui pourrait avoir un impact juridique ou tout aussi négatif sur elles, uniquement si cela s'avère nécessaire pour conclure ou exécuter un contrat ou si elles y ont consenti. Cette décision automatisée peut inclure le profilage dans certains cas, par ex. le traitement des données à caractère personnel qui évalue les caractéristiques de personnalité individuelles (par ex. solvabilité). Dans ce cas, la personne concernée doit être informée de la mise en œuvre d'une prise de décision individuelle automatisée et avoir l'opportunité de bénéficier d'une étude individuelle par un responsable du traitement.

5.6 Obligation d'information/ Transparence

Le secteur spécialisé responsable doit informer les personnes concernées de la finalité et des conditions du traitement de leurs données à caractère personnel conformément aux articles 13 et 14 du RGPD. Lorsque lesdites données ne relèvent pas du champ d'application du RGPD, l'information doit s'effectuer conformément au droit national applicable. L'information doit s'effectuer sous une forme précise, transparente et facile d'accès, ainsi que dans une langue claire et simple. Il convient de respecter les directives du délégué à la protection des données au sein du Groupe et de Data Compliance. Ces informations doivent être communiquées chaque fois que les données à caractère personnel sont collectées pour la première fois. Si la société du Groupe reçoit les données à caractère personnel d'un tiers, elle devra fournir les informations à la personne concernée dans un délai raisonnable après obtention des données sauf si

- la personne concernée détient déjà l'information ou
- s'il s'avère impossible ou
- extrêmement difficile de fournir cette information.

5.7 Limitation à une finalité spécifique

Les données à caractère personnel ne peuvent être traitées qu'à des fins légitimes définies avant la collecte des données. Toute modification de la finalité du traitement ne sera autorisée qu'à condition que le traitement soit compatible avec la finalité initiale de la collecte de données à caractère personnel.

5.8 Minimisation des données

Tout traitement des données à caractère personnel devra être limité, d'un point de vue aussi bien quantitatif que qualitatif, à ce qui est strictement nécessaire pour atteindre les objectifs visés par le traitement légal des données. Ce point doit être pris en compte lors de la collecte initiale des données. Si la finalité le permet et que l'effort s'avère proportionnel à l'objectif visé, il conviendra d'utiliser des données anonymisées ou statistiques.

5.9 Exactitude des données

Les données à caractère personnel enregistrées doivent être objectivement correctes et, si nécessaire, à jour. Le secteur spécialisé est tenu d'adopter des mesures appropriées pour garantir la suppression, la correction, l'extension ou la mise à jour des données collectées.

5.10 Privacy by Design (protection dès la conception) & Privacy by Default (protection par défaut)

Le principe « Privacy by Design » (protection des données dès la conception) vise à garantir le fait que les secteurs spécialisés définissent des stratégies internes modernes et adoptent des mesures pour intégrer les principes de protection des données dans les spécifications et l'architecture des modèles commerciaux/processus et des systèmes informatiques pour le traitement des données dès le début, à savoir dès la phase de conceptualisation et le concept technique. Conformément au principe de respect de la vie privée dès la conception, les procédures et les systèmes de traitement des données à caractère personnel devront être conçus de manière à restreindre leurs paramètres par défaut au traitement des données nécessaire à la réalisation de l'objectif (principe « protection des données par défaut »). Cela inclut le champ de traitement, le délai de stockage et l'accessibilité. Des mesures supplémentaires peuvent inclure :

- la pseudonymisation des données à caractère personnel dès que possible
- la transparence sur les fonctions et le traitement des données à caractère personnel
- l'autorisation accordée aux personnes concernées de décider du traitement de leurs données à caractère personnel
- la mise en capacité des opérateurs de procédures et de systèmes de concevoir et améliorer les fonctions de sécurité.

Toute société du Groupe devra implémenter et entretenir des mesures techniques et organisationnelles appropriées sur tout le cycle de vie de ses activités de traitement afin de s'assurer que les principes susmentionnés sont en permanence respectés.

5.11 Suppression et anonymisation

Les données à caractère personnel ne pourront être stockées que sur la période nécessaire à la réalisation de l'objectif visé par le traitement des données. Autrement dit, les données à caractère personnel devront être supprimées ou anonymisées dès que la finalité de leur traitement aura été atteinte ou n'aura plus lieu d'être, à moins qu'il ne persiste une obligation de conservation ou de documentation justificative. Les responsables des procédures individuelles doivent s'assurer de la mise en œuvre de la suppression et des routines d'anonymisation pour leurs procédures. Chaque système doit être doté d'une routine de suppression manuelle ou automatisée. Les demandes de suppression de la part des personnes concernées via la suppression ou l'effacement des identifiants personnels doivent être techniquement réalisables dans les systèmes. Les exigences imposées par Mercedes-Benz Group AG pour l'exécution des routines de suppressions (telles que les outils logiciels, les documents sur la mise en œuvre des concepts de suppression, les exigences de documentation) devront être respectées.

5.12 Sécurité du traitement

Les données à caractère personnel devront être protégées de tout accès non autorisé et traitement ou transfert illégal, de même que des pertes, altération et destruction accidentelles. Avant toute introduction de nouvelles méthodes de traitement des données, et en particulier de nouveaux systèmes informatiques, il conviendra de définir et de mettre en œuvre des mesures techniques et organisationnelles pour protéger les données à caractère personnel. Ces mesures doivent être basées sur l'état des connaissances, les risques de traitement et le besoin de protéger les données.

Les mesures techniques et organisationnelles nécessaires à la protection des données doivent être documentées par le responsable du traitement dans le contexte de l'évaluation de l'impact de la protection des données et du registre des processus.

En particulier, le secteur spécialisé concerné doit consulter son Responsable de la sécurité de l'information de l'entreprise (Business Information Security Officer (BISO)), son Responsable de la sécurité de l'information (Information Security Officer (ISO)) et son Réseau de protection

des données. Les exigences des mesures techniques et organisationnelles de protection des données s'inscrivent dans le cadre de la Gestion de la sécurité des informations de l'entreprise (Corporate Information Security Management) et doivent être constamment ajustées en fonction des évolutions techniques et des changements organisationnels.

5.13 Transmission (ultérieure) hors de Mercedes-Benz Group

La transmission des données à caractère personnel à des destinataires à l'extérieur ou à l'intérieur des sociétés du Groupe est soumise aux exigences d'autorisation concernant le traitement des données à caractère personnel de cette Section 5. Le destinataire des données doit en outre s'engager à n'utiliser ces données qu'aux fins définies.

En cas de transfert transfrontalier de données à caractère personnel (incluant l'autorisation d'accès de la part d'un autre pays), les exigences nationales concernant la transmission de données à caractère personnel vers un pays étranger doivent être respectées. En particulier, les données à caractère personnel issues de l'UE/ l'EEE ne pourront être traitées hors des sociétés du Groupe dans un pays tiers que si le destinataire peut prouver qu'il possède un niveau de protection des données équivalent à celui préconisé par la présente directive. Voici quelques moyens de preuve appropriés :

- Clauses contractuelles types UE,
- Participation du destinataire à un système de certification accrédité UE pour garantir un niveau de protection des données approprié ou
- Reconnaissance des règles d'entreprises contraignantes pour créer un niveau de protection des données adéquat par l'autorité de contrôle responsable.

Les transferts de données à caractère personnel à une autorité publique ne pourront être massifs, disproportionnés et systématiques, autrement dit excéder ce qui est nécessaire dans une société démocratique. En cas de conflit entre ceux-ci et les exigences de l'autorité publique, Mercedes-Benz Group AG collaborera avec la société du Groupe responsable pour trouver une solution pratique qui répond à la finalité de la présente directive (Section 14.3).

Toutes les obligations définies dans la présente Section 5 sont des droit du tiers bénéficiaire pour la personne concernée.

6 Analyse d'impact relative à la protection des données

Lorsqu'elles introduiront de nouveaux traitements ou en cas de modification significative du traitement existant avant ledit traitement, en particulier du fait de l'utilisation de nouvelles technologies, les sociétés du Groupe devront évaluer si ce traitement représente un risque élevé pour la vie privé des personnes concernées. La nature, l'étendue, le contexte et la finalité du traitement des données devront être pris en compte. Dans le cadre de l'analyse de risques, le secteur spécialisé responsable réalisera une évaluation de l'impact du traitement planifié sur la protection des données à caractère personnel (Analyse d'impact relative à la protection des données). Si, après analyse d'impact relative à la protection des données et application des mesures de réduction des risques appropriées, il apparaît que le risque pour les droits et les libertés des personnes concernées est élevé, le délégué à la protection des données au sein du Groupe devra en être informé de manière à pouvoir consulter l'autorité de contrôle de la protection des données. Les dispositions établies par Mercedes-Benz Group AG pour la réalisation de l'analyse d'impact relative à la protection des données (telles que les outils logiciels, les instructions sur la réalisation de l'évaluation) devront être respectées.

7 Documentation des procédures de traitement

Chaque société du Groupe doit documenter les procédures impliquant le traitement de données à caractère personnel dans un registre des procédures. Le registre des procédures doit être tenu par écrit, si nécessaire dans un format électronique, et mis à la disposition de l'autorité de contrôle de la protection des données sur simple demande. Les dispositions établies par Mercedes-Benz Group AG pour la documentation (telles que les outils logiciels et les instructions sur la documentation) devront être respectées.

8 Traitement pour le compte du responsable

8.1 Informations générales

Un traitement sur commande voit le jour lorsqu'un preneur d'ordre traite des données à caractère personnel en tant que prestataire de service au nom et sur ordre du donneur d'ordre. Dans ce cas, un accord relatif à la sous-traitance de traitement de données à caractère personnel doit être conclu avec les sous-traitants externes, ainsi qu'avec les sociétés du Groupe au sein de Mercedes-Benz Group AG conformément aux exigences légales applicables (par ex. « Accord relatif à la sous-traitance du traitement des données à caractère personnel »). Le responsable du traitement des données est pleinement responsable de la réalisation correcte du traitement des données.

Les dispositions de la Section 8.3. s'appliquent aussi aux donneurs d'ordre externes qui ne sont pas des sociétés du Groupe.

8.2 Dispositions pour les responsables du traitement des données

Lorsque la commande est émise, les exigences suivantes doivent être respectées, le secteur spécialisé passant la commande devant s'assurer qu'elles sont bien remplies :

- Le preneur d'ordre doit être sélectionné en fonction de son aptitude à garantir la mise en œuvre des mesures de protection d'ordre technique et organisationnel indispensables.
- Les standards contractuels pour la protection des données fournis par le délégué à la protection des données du Groupe doivent être respectés.
- La commande doit être passée par écrit ou sous forme électronique. Les instructions à respecter dans le cadre du traitement des données et la répartition des responsabilités entre le donneur d'ordre et le preneur d'ordre doivent être stipulées dans des documents dûment archivés.

Le donneur d'ordre doit s'assurer dès le début du traitement des données par un test approprié que le preneur d'ordre remplit les obligations précitées. Les dispositions établies par Mercedes-Benz Group AG à cet égard (telles que les outils logiciels et les instructions sur la mise en œuvre de l'évaluation, modèle de contrat) devront être respectées. Un sous-traitant peut documenter sa conformité aux exigences en matière de protection des données, en particulier en présentant une certification appropriée. Selon le risque présenté par le traitement des données, les vérifications devront être répétées sur une base régulière pendant toute la durée du contrat.

8.3 Disposition pour les sous-traitants internes

Le sous-traitant ne peut traiter les données à caractère personnel que suivant les instructions du responsable du traitement.

Les sous-traitants internes ne pourront engager d'autres sociétés du Groupe ou tiers (« autres sous-traitants ») pour traiter les données à caractère personnel dans leur propre (sous-)contrat qu'avec le consentement préalable du responsable du traitement. Ce consentement ne sera accordé que si le sous-traitant soumet l'autre sous-traitant – par contrat ou par d'autres moyens légalement contraignants comparables, aux mêmes obligations en termes de protection des données que celles du sous-traitant lui-même, conformément à la présente directive, à l'égard de la société du Groupe et des personnes concernées. Il doit également obliger l'autre sous-traitant à prendre les mesures de protection techniques et organisationnelles appropriées. Le type de consentement, ainsi que les obligations d'information en cas de modification de la relation sous-traitée devront être définis dans le contrat de services.

Les sous-traitants sont tenus de fournir l'aide appropriée au responsable du traitement en matière de respect des dispositions relatives à la protection des données applicables à ce dernier, en particulier en fournissant toutes les informations nécessaires. Cela concerne en particulier la sauvegarde des éléments suivants :

- principes généraux de traitement conformément à la Section 5
- droits des personnes concernées conformément à la Section 10
- obligations de notification des incidents en termes de protection des données conformément à la Section 12
- dispositions concernant le responsable du traitement et les sous-traitants conformément à la Section 8
- et la gestion des demandes et des enquêtes par les autorités de contrôle.

Si des standards applicables ou des dispositions légales exigent du sous-traitant d'effectuer le traitement contrairement aux instructions du responsable du traitement, si ces dispositions empêchent le sous-traitant de remplir ses obligations aux termes de la présente directive ou de l'accord sur le traitement pour le compte du responsable du traitement, le sous-traitant devra immédiatement en informer son responsable de traitement sauf si la disposition légale concernée interdit ce type de notification. La disposition s'applique de manière correspondante si le sous-traitant n'est pas en mesure de se conformer aux instructions de son responsable de traitement pour d'autres raisons. Dans ce cas, le responsable du traitement a le droit de suspendre la transmission des données et/ou de mettre fin à l'accord relatif à la sous-traitance de traitement de données à caractère personnel.

Les sous-traitants sont tenus de notifier à leurs responsables de traitement toute demande légalement contraignante émanant d'autorités publiques concernant la communication de données à caractère personnel sauf si cela leur est interdit pour d'autres raisons.

Selon le choix du responsable du traitement, le sous-traitant doit supprimer ou retourner toutes les données à caractère personnel fournies par le responsable du traitement dès la prestation de service terminée.

Les sous-traitants sont tenus d'informer immédiatement leur responsable de traitement et, le cas échéant, le client de leur responsable de traitement, de tout recours, requête ou réclamation émanant des personnes concernées.

Les responsables de traitement internes du Groupe doivent également obliger les sous-traitants externes à se conformer aux règlements susmentionnés.

Les obligations spécifiques du sous-traitant envers le responsable du traitement sont des droits du tiers bénéficiaire pour la personne concernée.

9 Responsabilité conjointe du traitement

Dans le cas où de multiples sociétés du Groupe définiraient conjointement la finalité du traitement des données à caractère personnel (de même qu'avec un ou plusieurs tiers, le cas échéant) (responsables conjoints du traitement), les entreprises doivent conclure un accord qui stipule leurs obligations et leurs responsabilités vis-à-vis de la personne concernée dont ils traitent les données. Les modèles de contrats types fournis par le délégué à la protection des données du Groupe doivent être respectés.

10 Droits exécutoires des personnes concernées

Tous les droits des personnes concernées et les obligations des sociétés du Groupe définis dans la présente Section 10 sont des droits du tiers bénéficiaire pour la personne concernée.

Les demandes et les réclamations transmises conformément à la présente Section 10 doivent généralement appeler une réponse dans un délai d'un mois. Compte tenu de la complexité et du nombre de demandes, ce délai d'un mois pourra être prolongé de deux mois maxi et la personne concernée devra en être informée.

10.1 Droits des personnes concernées

Une personne concernée dans l'UE/ EEE a les droits suivants, tels que spécifiés plus en détail dans la législation UE vis-à-vis de la société du Groupe responsable ou – si la société du Groupe est le sous-traitant – vis-à-vis du responsable du traitement :

- Droit d'être informé des circonstances du traitement de ses données à caractère personnel . Les exigences du délégué à la protection des données du Groupe concernant ces informations doivent être respectées.
- Droit d'obtenir des informations sur les modalités de traitement de ses données et les droits dont elle dispose dans ce contexte. Si, dans le cadre d'une relation de travail, la législation du travail respective prévoit un droit de regard spécifique sur les informations conservées par l'employeur (dossiers personnels des collaborateurs), ce droit est intégralement préservé.Sur simple demande, la personne concernée pourra recevoir une copie de ses données à caractère personnel (éventuellement contre une somme raisonnable), sauf si les intérêts des tiers dignes de protection s'y opposent.
- Droit de corriger ou compléter les données à caractère personnel si celles-ci sont incorrectes ou incomplètes.
- Droit à l'effacement de ses données à caractère personnel si elle retire son consentement ou si la base légale du traitement a cessé de s'appliquer. Il en va de même si la finalité du traitement des données a expiré ou cessé de s'appliquer pour d'autres raisons. Les délais de conservation et les intérêts dignes de protection qui interdisent l'effacement doivent être respectés.
- Droit à la limitation du traitement de ses données si elle conteste leur exactitude ou si la société du Groupe n'a plus besoin des données tandis que la personne concernée a besoin des données pour faire valoir un droit en justice. La personne concernée peut aussi demander que la société du Groupe limite le traitement de ses données si une suppression de ces données est nécessaire ou si un examen d'une objection émise par la personne concernée est en cours.
- Droit de réception des données à caractère personnel la concernant qu'elle a fournies sur la base du consentement ou dans le contexte d'un accord conclu ou initié avec elle dans un format numérique usuel. Elle est aussi habilitée à transmettre ces données à un tiers lorsque le traitement est effectué à l'aide de procédés automatisés et que cela s'avère techniquement possible.

- Droit de s'opposer à tout moment au marketing direct. Un système de gestion adéquate du consentement et de l'opposition doit être assuré.
- Droit de s'opposer au traitement des données à caractère personnel sur la base légale d'intérêts supérieurs d'une société du Groupe ou d'un tiers pour des raisons liées à sa situation personnelle particulière. Cependant, ce droit d'opposition ne s'applique pas si la société du Groupe a des raisons impérieuses de traiter les données ou si les données sont traitées pour la constatation, l'exercice ou la défense de droits en justice. S'il existe une objection légitime, les données devront être supprimées.

De plus, la personne concernée est également habilitée à faire valoir ses droits à l'encontre de la société du Groupe important les données dans un pays tiers.

10.2 Procédure de réclamation

Les personnes concernées sont en droit d'adresser une réclamation au délégué à la protection des données au sein du Groupe si elles ont le sentiment que la présente directive a été enfreinte. Les réclamations de ce type peuvent être transmises par e-mail.

La société du Groupe établie dans l'UE/ EEE qui exporte les données assistera les personnes concernées dont les données à caractère personnel ont été collectées dans l'UE/ EEE en établissant les faits et en faisant valoir leurs droits aux termes de la présente directive à l'encontre de la société du Groupe qui importe les données.

Au cas où une personne concernée serait en désaccord avec une décision d'une société du Groupe concernant le respect de ces exigences (ou si elle n'est pas satisfaite de sa conduite), elle est libre de contester cette décision ou conduite en exerçant ses droits. A cette fin, elle peut s'adresser à l'autorité de contrôle compétente, en particulier dans le pays de son lieu de résidence habituel, de son lieu de travail ou du lieu de l'infraction présumée ou porter une action en justice (Section 11.2). Les autres droits et responsabilités juridiques ne s'en trouvent pas affectés.

11 Responsabilité et lieu de juridiction

11.1 Clauses de responsabilité

La société du Groupe établie dans l'UE/ EEE (« exportateur de données ») qui a initialement transféré les données à caractère personnel à une société du Groupe établie dans un pays tiers répondra de toute violation de la présente directive par ladite société du Groupe basée dans un pays tiers qui reçoit des données de l'UE/ EEE pour traitement dans le pays tiers. Cette responsabilité inclut l'obligation de remédier à des situations illégales, ainsi que d'indemniser le dommage matériel et immatériel causé par une violation de la présente directive par les sociétés du Groupe implantées dans un pays tiers.

L'exportateur de données ne sera exonéré en partie ou intégralement de cette responsabilité que s'il peut prouver que la société du Groupe du pays tiers qui reçoit les données de l'UE/ EEE n'est pas responsable de l'action qui a causé le dommage.

11.2 Lieu de juridiction

Toute personne concernée peut intenter une action en justice devant les tribunaux du siège du responsable du traitement ou du sous-traitant ou encore de son lieu de résidence habituel.

Toute personne concernée qui dénonce un manquement à la présente directive dans le cadre d'un traitement dans un pays tiers peut faire valoir ses droits contre à la fois l'entreprise important des données et celle exportant des données dans l'UE/ EEE. Par conséquent, la personne concernée peut porter l'infraction alléguée et les demandes en justice qui en découlent devant les tribunaux et les autorités de contrôle compétents, soit au siège du responsable du traitement, soit à sa résidence habituelle.

Les dispositions relatives à la responsabilité et au lieu de juridiction dans cette Section sont des droits du tiers bénéficiaire pour la personne concernée.

12 Notification des incidents en matière de protection des données

En cas de manquement potentiel aux exigences en matière de sécurité des données (« incident en matière de protection des données »), les sociétés du Groupe impliquées ont des obligations d'enquête, d'information et d'atténuation des dommages. Un incident en matière de protection des données est une violation des données s'il existe une violation de la sécurité induisant une destruction illicite, une altération, une divulgation non autorisée ou l'utilisation illicite de données à caractère personnel. Lorsque la violation en matière de données personnelles est susceptible de se traduire par un risque élevé pour les droits et les libertés des personnes physiques, l'autorité de contrôle devra être informée de l'infraction correspondante si possible dans les 72 heures qui suivent la détection initiale. De plus, les personnes concernées doivent être informées de toute violation des données personnelles susceptible de présenter un risque élevé pour leurs droits et leurs libertés. Les sous-traitants tels que définis à la Section 8.2 sont tenus de rapporter immédiatement les incidents en matière de protection des données à leur donneur d'ordre.

Si un incident en matière de protection des données a été identifié ou suspecté dans le champ de responsabilité d'une société du Groupe, tous les collaborateurs sont priés de le rapporter immédiatement, conformément au processus de gestion des incidents de sécurité de l'information. Les dispositions établies par Mercedes-Benz Group AG à cet égard (telles que les outils logiciels et les instructions sur la mise en œuvre de la notification) devront être respectées.

Tout incident en matière de protection des données doit être documenté et la documentation doit être mise à la disposition de l'autorité de contrôle sur simple demande.

13 Organisation de la protection des données et sanctions

13.1 Responsabilité :

Les membres des organes de gestion des sociétés du Groupe sont responsables du traitement des données dans leur domaine de responsabilité. Ils sont donc tenus de veiller à ce que les exigences légales et les dispositions relatives à la protection des données mentionnées dans la présente directive sur la protection des données UE soient respectées (par ex. les obligations nationales en matière de reporting).Dans son domaine de responsabilité, l'équipe de direction est chargée de s'assurer que les mesures organisationnelles, RH et techniques sont en place pour que tout traitement de données soit réalisé en conformité avec les exigences en matière de protection des données. La conformité à ces exigences relève de la responsabilité des collaborateurs concernés. En cas de contrôles de sécurité des données par une autorité publique, le délégué à la protection des données au sein du Groupe doit être informé immédiatement.

13.2 Sensibilisation et formation

La Direction doit s'assurer que ses collaborateurs reçoivent la formation requise en matière de protection des données, incluant le contenu et la gestion de la présente directive, et y assistent s'ils ont un accès permanent ou fréquent aux données à caractère personnel ou qu'ils sont impliqués dans la collecte de données ou dans le développement d'outils de traitement des données à caractère personnel. Il convient de respecter les directives du délégué à la protection des données au sein du Groupe et de Data Compliance.

13.3 Organisation

Le délégué à la protection des données du Groupe n'est soumis à aucune instruction en interne concernant la réalisation de ses tâches. Il doit assurer la conformité aux lois sur la protection des données nationales et internationales. Il est responsable de la présente directive et contrôle son respect. Lorsque des sociétés du Groupe souhaitent participer à un système de certification international concernant les règles d'entreprise contraignantes en matière de protection des données, elles doivent demander au responsable de la protection des données du Groupe de valider leur participation.

Le délégué la protection des données au sein du Groupe est désigné par le Directoire de Mercedes-Benz Group AG et soutenu dans la réalisation de ses tâches par ce dernier. Généralement, les sociétés du Groupe légalement tenues de nommer un responsable de la protection des données désigneront le délégué à la protection des données du Groupe. Le délégué à la protection des données au sein du Groupe rapporte directement au Directoire de Mercedes-Benz Group AG et à la direction respective de toutes les sociétés du Groupe pour lesquelles le délégué à la protection des données du Groupe a été nommé. Les exceptions spécifiques doivent être examinées avec le délégué à la protection des données du Groupe.

Le conseil de surveillance de Mercedes-Benz Group AG doit être informé dans le cadre des obligations de reporting existantes via un rapport annuel du délégué à la protection des données du Groupe.

Toutes les personnes concernées peuvent contacter le délégué à la protection des données du Groupe à tout moment pour exprimer leurs préoccupations, poser des questions, demander un complément d'information ou soumettre des réclamations relatives à la protection ou à la sécurité des données. Si cela est souhaité, les sujets de préoccupation et les réclamations seront traités avec confidentialité.

Les coordonnées du délégué à la protection des données du Groupe sont :

Mercedes-Benz Group AG, Konzernbeauftragter für den Datenschutz, HPC E600,
70546 Stuttgart, Allemagne
E-mail : data.protection@mercedes-benz.com
Intranet : https://social.intra.corpintra.net/docs/DOC-71499

Mercedes-Benz Group a en outre mis en place une organisation Compliance décrite plus en détail par des règlements internes séparés. L'organisation Compliance aide et supervise les sociétés du Groupe en matière de conformité aux lois sur la protection des données. Elle définit le contenu des formations sur la protection des données et stipule les critères pour le groupe de participants.

13.4 Sanctions

Le traitement illicite des données à caractère personnel ou autres manquements à la législation sur la protection des données peut être poursuivi en justice en vertu des réglementations et des lois pénales en vigueur dans de nombreux pays et peut aussi conduire à des demandes d'indemnisation. Les infractions dont les collaborateurs sont responsables individuellement peuvent entraîner des actions disciplinaires en vertu de la législation du travail. Les violations de la présente directive feront l'objet de sanctions pénales conformément aux règlements internes.

13.5 Audits et contrôles

La conformité à la présente directive et aux lois sur la protection des données applicables sera régulièrement réexaminée à l'échelle du Groupe - et ce, au moins une fois par an – sur la base des risques. Ce contrôle sera effectué via une évaluation interne des risques de compliance, des audits incluant des thèmes spécifiques à la protection des données et autres contrôles. Le délégué à la protection des données du Groupe a le droit d'exiger d'autres contrôles. Les résultats devront être rapportés au délégué à la protection des données du Groupe, à la société du Groupe responsable et à son délégué à la protection des données, si ce dernier a été désigné.

Le Directoire de Mercedes-Benz Group AG devra être informé des résultats dans le cadre des obligations de reporting existantes. Les résultats des contrôles seront mis à disposition de l'autorité de contrôle de la protection des données compétente, sur simple demande. Dans le cadre des attributions qui lui ont été octroyées en vertu du droit national, l'autorité de contrôle de la protection des données compétente peut également procéder à ses propres audits en matière de protection des données afin de vérifier le respect des dispositions de la présente directive.

14 Amendements de la présente directive et collaboration avec les autorités

14.1 Responsabilités en cas d'amendements

La directive ne pourra être modifiée que via la procédure définie pour l'amendement des directives en coordination avec le délégué à la protection des données du Groupe (Directive sur la gestion des directives A1). Les modifications qui ont un effet significatif sur la présente directive sur la protection des données UE, A 17 ou affectent le niveau de protection offert par ladite directive (par ex. modifications de son caractère contraignant) devront être rapidement rapportées aux autorités de contrôle compétentes qui valident la présente directive comme règle d'entreprise contraignante.

Le délégué à la protection des données du Groupe est chargé de tenir une liste de toutes les sociétés du Groupe relevant de la présente directive (Autre règlement applicable « Liste des sociétés du Groupe relevant de la directive sur la protection des données UE »). Aucun transfert de données à caractère personnel à une nouvelle société du Groupe ne sera effectué sur la base de la présente directive tant que ladite société ne sera pas rattachée de manière effective à cette directive et que les mesures de compliance correspondantes visant au respect de la directive ne seront pas prises en compte.

La personne concernée a le droit de disposer d'un accès aisé à la présente directive. C'est pourquoi la dernière version de cette directive est publiée sur Internet à l'adresse https://www.group.mercedes-benz.com, sous la rubrique Protection des données. Cette exigence est un droit du tiers bénéficiaire pour la personne concernée.

Si des amendements sont apportés à la présente directive ou à la liste des sociétés affiliées au Groupe, l'autorité de contrôle de la succursale principale de Mercedes-Benz Group AG en sera informée une fois par an par le délégué à la protection des données du Groupe et les raisons de cette actualisation lui seront brièvement exposées.

14.2 Collaboration avec les autorités

Les sociétés du Groupe qui procèdent ou participent au traitement dans des pays tiers sont tenues de collaborer avec l'autorité de contrôle responsable pour toutes les questions relatives aux difficultés, requêtes et autres procédures en lien avec le traitement des données à caractère personnel dans le contexte mentionné ci-dessus. Cela inclut l'obligation d'accepter les audits légaux réalisés par les autorités de contrôle. De plus, il conviendra de respecter les instructions légales émises par les autorités de contrôle responsables basées sur ou en lien avec les procédures de traitement dans les pays tiers ou les dispositions de la présente directive.

Les dispositions de la Section 14.2 sur la collaboration avec les autorités sont des droits du tiers bénéficiaire pour la personne concernée.

14.3 Suivi et reporting des réglementations des pays tiers

Les responsables du traitement des données dans les entreprises de pays tiers doivent informer sans délai le délégué à la protection des données du Groupe si leur entreprise a des motifs raisonnables de croire que des lois ou d'autres réglementations non émises par l'UE en tant qu'institution ou par l'un de ses Etats membres comportent les risques suivants :

- les lois ou réglementations sont telles qu'elles peuvent empêcher la société du pays tiers concernée ou une autre société du Groupe de remplir ses obligations aux termes de la présente directive lors du traitement des données dans les pays tiers ou
- les lois ou réglementations peuvent produire des effets néfastes significatifs sur les droits dont bénéficient les personnes concernées aux termes de la présente directive pour le traitement des données dans les pays tiers. En particulier si l'autorité publique locale demande un transfert de données à caractère personnel massif, disproportionné et systématique, autrement dit excédant ce qui est nécessaire dans une société démocratique.

Le délégué à la protection des données du Groupe évaluera l'impact et informera l'autorité de protection des données compétente (le cas échéant) si les exigences légales concernées sont amenées à interférer d'une manière significative avec les garanties accordées par la présente directive. Cette disposition est un droit du tiers bénéficiaire pour la personne concernée.

Si une société d'un pays tiers est priée par une autorité publique de s'abstenir de notifier la communication des données à caractère personnel à l'autorité de contrôle de la protection des données, elle devra prendre toutes les mesures appropriées pour atténuer autant que possible cette interdiction ou l'abroger et fournir une fois par an des informations générales sur les demandes reçues aux autorités de contrôle compétentes dans le cadre prescrit (par ex. nombre de demandes de communication, type de données demandées, demandeur si possible).

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