仮日本語訳

Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications

Version 2.0

Adopted on 9 March 2021

コネクテッドビークル及びモビリティ関連アプリケーションにおける個人データの取扱いに関するガイドライン01/2020

バージョン 2. 0

2021年3月9日に採択

本書面は、The European Data Protection Board（欧州データ保護会議）により2021年3月9日に採択された“Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications” を個人情報保護委員会が翻訳したものである。本書面は参考のための仮日本語訳であって、その利用について当委員会は責任を負わないものとし、正確な内容については原文を参照されたい。

Version history
バージョン履歴

Version 2.0 バージョン 2. 0	9 March 2021 2021年3月9日	Adoption of the Guidelines after public consultation パブリック・コンサルテーション後におけるガイドラインの採択
Version 1.0 バージョン 1. 0	28 January 2020 2020年1月28日	Adoption of the Guidelines for public consultation パブリック・コンサルテーションのためのガイドラインの採択

Table of contents
目次

The European Data Protection Board
欧州データ保護会議は、

Having regard to Article 70 (1) (e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),
個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令95/46/ECを廃止する欧州議会及び理事会の2016年4月27日の規則(EU)2016/679（以下「GDPR」という）の第70条(1)(e)に鑑み、

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],
2018年7月6日のEEA共同委員会の決定No 154/2018により改正されたEEA協定[1]、特にその附属書XI及び議定書37に鑑み、

Having regard to Article 12 and Article 22 of its Rules of Procedure,
その手続規則の第12条及び第22条に鑑み、

HAS ADOPTED THE FOLLOWING GUIDELINES
以下のガイドラインを採択する。

1 INTRODUCTION
はじめに

1. Symbol of the 20th century economy, the automobile is one of the mass consumer products that has impacted society as a whole. Commonly associated with the notion of freedom, cars are often considered as more than just a means of transportation. Indeed, they represent a private area in which people can enjoy a form of autonomy of decision, without encountering any external interferences. Today, as connected vehicles move into the mainstream, such a vision no longer corresponds to the reality. In-vehicle connectivity is rapidly expanding from luxury models and premium brands to high-volume midmarket models, and vehicles are becoming massive data hubs. Not only vehicles, but drivers and passengers are also becoming more and more connected. As a matter of fact, many models launched over the past few years on the market integrate sensors and connected on-board equipment, which may collect and record, among other things, the engine performance, the driving habits, the locations visited, and potentially even the driver's eye movements, his or her pulse, or biometric data for the purpose of uniquely identifying a natural person[2].
20世紀の経済の象徴である自動車は、社会全体に大きな影響を及ぼした大衆向け消費財の一つである。自動車は、一般に自由という概念と結び付けられ、単なる輸送手段以上のものであるとみなされる場合が多い。実際自動車は、人々が、外部からの干渉にさらされることなく、ある種の自己決定を享受できるプライベートな空間を象徴している。今日、コネクテッドビークルが主流になるにつれ、このようなイメージは現実にそぐわないものとなっている。コネクティビティ搭載車両が高級

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
本ガイドラインにおいて、「加盟国」という表現は、「EEA加盟国」と解釈されたい。

モデルやプレミアムブランドの車から量販の中級モデルへと急速に拡大しており、車両が巨大なデータハブになりつつある。また、車両のみならず、運転者と同乗者もますます接続性を増している。実際のところ、過去数年間に市場に投入された多くのモデルには、センサーや接続された車載機器が組み込まれており、特にエンジンの性能、運転習慣、訪問先の情報を収集し、記録することができるほか、潜在的には運転者の眼球の動き、脈拍又は自然人を一意に識別することを目的とする生体データさえ収集し、記録することができるようになっている[2]。

2. Such data processing is taking place in a complex ecosystem, which is not limited to the traditional players of the automotive industry, but is also shaped by the emergence of new players belonging to the digital economy. These new players may offer infotainment services such as online music, road condition and traffic information, or provide driving assistance systems and services, such as autopilot software, vehicle condition updates, usage-based insurance or dynamic mapping. Moreover, since vehicles are connected via electronic communication networks, road infrastructure managers and telecommunications operators involved in this process also play an important role with respect to the potential processing operations applied to the drivers' and passengers' personal data.
そのようなデータの取扱いは複雑なエコシステムの中で行われており、当該エコシステムは自動車業界の従来の参加者だけではなく、デジタル経済に属する新たな参加者も加え形作られている。これらの新たな参加者は、オンラインミュージック、道路状況、交通情報などのインフォテインメント（infotainment）・サービスを提供する場合もあれば、オートパイロットソフトウェア、車両状態最新情報サービス、利用ベース型の保険、又はダイナミックマップなどの運転支援システム及びサービスを提供する場合もある。さらに、車両が電子通信ネットワークを介して接続されているため、当該過程に関与する道路インフラの管理者及び情報通信事業者も、運転者及び同乗者の個人データについて行われることになる取扱業務に関連して重要な役割を果たす。

3. In addition, connected vehicles are generating increasing amounts of data, most of which can be considered personal data since they will relate to drivers or passengers. Even if the data collected by a connected car are not directly linked to a name, but to technical aspects and features of the vehicle, it will concern the driver or the passengers of the car. As an illustration, data relating to the driving style or the distance covered, data relating to the wear and tear on vehicle parts, location data or data collected by cameras may concern driver behaviour as well as information about other people who could be inside or data subjects that pass by. Such technical data are produced by a natural person, and permit his/her direct or indirect identification, by the data controller or by another person. The vehicle can be considered as a terminal that can be used by different users. Therefore, as for a personal computer, this potential plurality of users does not affect the personal nature of the data.
加えて、コネクテッドビークルから生成されるデータの量は増え続けており、その大半は運転者又は同乗者に関連するものであるため、個人データとみなすことができる。コネクテッドビークルにより収集されるデータを氏名に直結させず、車両の技術的側面や特徴に結び付けている場合でも、当該データは車両の運転者又は同乗者に関わるものと考えられる。一例として、運転スタイル又は走行距離に関するデータ、車両部品の摩耗に関するデータ、位置データ又はカメラにより収集されるデ

[2] Infographic "Data and the connected car" by the Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf
Future of Privacy Forumによるインフォグラフィック、「データとコネクテッドカー」、https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

ータが運転者の行動を示す場合もあれば、車両内にいる可能性のある他の人々又は通りすがりのデータ主体の情報を示す場合もある。このような技術データは自然人からもたらされ、データ管理者又はその他の者が当該自然人を直接的又は間接的に識別可能にする。車両は、多様なユーザーが利用できる端末とみなすことができる。したがって、パーソナルコンピュータの場合と同様、このように複数のユーザーに利用される可能性があってもデータの個人性は損なわれない。

4. In 2016, the Fédération Internationale de l'Automobile (FIA) ran a campaign across Europe called "My Car My Data" to get a sentiment on what Europeans think about connected cars[3]. While it showed the high interest of drivers for connectivity, it also highlighted the vigilance that must be exercised with regard to the use of the data produced by vehicles as well as the importance of complying with personal data protection legislation. Thus, the challenge is, for each stakeholder, to incorporate the "protection of personal data" dimension from the product design phase, and to ensure that car users enjoy transparency and control in relation to their data in accordance with recital 78 GDPR. Such an approach helps to strengthen user confidence, and thus the long-term development of those technologies.
国際自動車連盟（FIA）は2016年、コネクテッドビークルに関して欧州の人々が持つ感情を調べるために「マイカー・マイデータ（My Car My Data）」と呼ばれるキャンペーンを欧州全域で展開した[3]。その結果は、運転者がコネクティビティ機能に高い関心を有することを示す一方、車両により生成されるデータを極めて注意深く使用しなければならないこと、また個人データ保護法令を遵守する重要性を強調するものであった。従って、製品の設計段階から「個人データの保護」機能を組み込み、自動車の使用者がGDPR前文第78項に従い自己のデータに関する透明性とその管理を享受できるよう確保することが各ステークホルダーにとっての課題である。このようなアプローチは、使用者の信頼度を高め、ひいてはこれらの技術の長期的な発展の強化を促すものとなる。

1.1 Related works
関連の取組み

5. Connected vehicles have become a substantial subject for regulators over the last decade, with a major increase in the last couple of years. Various works have thus been published at the national and international levels concerning the security and privacy of connected vehicles. Those regulations and initiatives aim at complementing the existing data protection and privacy frameworks with sector specific rules or providing guidance to professionals.
コネクテッドビークルはこの10年間で規制当局にとって重要なテーマとなっており、特にこの数年、その傾向が著しい。したがって、コネクテッドビークルの安全管理及びプライバシーに関する国内及び国際レベルの多様な取組みが公表されている。これらの規制及びイニシアティブのねらいは、データ保護及びプライバシーに関する既存の枠組みを当該産業部門固有の規制で補完すること、又は専門家に向け指針を示すことにある。

1.1.1 European-level and international initiatives
欧州レベルのイニシアティブ及び国際的イニシアティブ

6. Since 31 March 2018, a 112-based eCall in-vehicle system is mandatory on all new types of M1 and N1 vehicles (passenger cars and light duty vehicles)[4, 5]. In 2006, the Article 29 Working Party had already adopted a working document on data protection and privacy implications in eCall initiative[6]. In addition, as previously discussed※, the Article 29 Working

[3] Campaign "My Car My Data"; http://www.mycarmydata.eu/.
「マイカー・マイデータ」キャンペーン、http://www.mycarmydata.eu/.

Party also adopted an opinion in October 2017 regarding the processing of personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).
2018年3月31日以降、112番eCall（緊急通報）車載システムをM1及びN1（乗用車及び小型車）の全新型車両に搭載することが義務付けられている[4,5]。第29条作業部会は2006年にeCallイニシアティブのデータ保護及びプライバシーへの影響に関する作業文書を既に採択している[6]。さらに、第29条作業部会は、前述のように※協調型高度道路交通システム（C-ITS）に関連する個人データの取扱いに関する意見を2017年10月に採択している。
※仮訳者注：C-ITSに関する第29条作業部会意見については、「後述の」パラグラフ36にて言及あり。

7. In January 2017, the European Union Agency for Network and Information Security (ENISA) published a study focused on cyber security and resilience of smart cars listing the sensitive assets as well as the corresponding threats, risks, mitigation factors and possible security measures to implement[7]. In September 2017, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) adopted a resolution on connected vehicles[8]. Finally, in April 2018, the International Working Group on Data Protection in Telecommunications (IWGDPT), also adopted a working paper on connected vehicles[9].
欧州ネットワーク・情報セキュリティ機関（ENISA）はスマートカーのサイバーセキュリティと強靭性に焦点をあてた調査の結果を2017年1月に発表し、その中でセンシティブな資産とそれに対応する脅威、リスク、軽減策、及び導入可能な安全管理措置を列記している[7]。データ保護プライバシー・コミッショナー国際会議（ICDPPC）は、コネクテッドビークルに関する決議を2017年9月に採択している[8]。
最後になるが、情報通信分野におけるデータ保護に関する国際ワーキンググループ（IWGDPT）も、コネクテッドビークルに関するワーキングペーパーを2018年4月に採択している[9]。

---

[4] The interoperable EU-wide eCall; https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.
「EU全域に及ぶ相互運用可能なeCall、https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.
[5] Decision No 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall service Text with EEA relevance; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0585.
「EU全域に及ぶ相互運用可能なeCallサービスの配備に関する2014年5月15日の欧州議会及び理事会の決定No 585/2014/EU」（EEA関連条文）、https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0585.
[6] Working document on data protection and privacy implications in eCall initiative; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf.
「eCallイニシアティブにおけるデータ保護及びそのプライバシーへの影響に関する作業文書」、http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf.
[7] Cyber security and resilience of smart cars; https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.
「スマートカーのサイバーセキュリティと強靭性」、https://www.enisa.europa.eu/publications/cyber-security-and- resilience-of-smart-cars.
[8] Resolution on data protection in automated and connected vehicles; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and- connected-vehicles_en_1.pdf.
「自動運転車及びコネクテッドビークルのデータ保護に関する決議」、https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and- connected-vehicles_en_1.pdf.
[9] Working paper on connected vehicles; https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/.
「コネクテッドビークルに関するワーキングペーパー」、https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/.

1.1.2 National initiatives of European Data Protection Board (EDPB) members
欧州データ保護会議（EDPB）メンバーの国内イニシアティブ

8. In January 2016, the Conference of the German Federal and State Data Protection Authorities and the German Association of the Automotive Industry (VDA) published a common declaration on the principles of data protection in connected and not-connected vehicles[10]. In August 2017, the UK Centre for Connected and Autonomous Vehicles (CCAV) released a guide stating principles of cyber security for connected and automated vehicles in order to raise awareness on the matter within the automotive sector[11]. In October 2017, the French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), released a compliance package for connected cars in order to provide assistance to stakeholders on how to integrate data protection by design and by default, enabling data subjects to have effective control over their data[12].
ドイツ連邦・州データ保護監督委員会（データ保護会議）とドイツ自動車工業会（VDA）は2016年1月、コネクテッドビークルと非コネクテッドビークルのデータ保護原則に関する共同宣言を発表した[10]。英国のコネクテッド・自動運転車センター（CCAV）は2017年8月、コネクテッドビークル及び自動運転車のサイバーセキュリティに関し、自動車業界の問題意識を喚起するため、当該原則を示した手引を発行した[11]。フランスのデータ保護機関である情報処理と自由に関する国家委員会（CNIL）は2017年10月、データ主体が自己のデータに対する効果的な管理を享受できるよう、データ保護バイデザイン及びデータ保護バイデフォルトを組み入れる方法について、ステークホルダーを支援することを目的とした、コネクテッドビークルに関する遵守パッケージを発表した[12]。

1.2 Applicable law
適用法

9. The relevant EU legal framework is the GDPR. It applies in any case where data processing in the context of connected vehicles involves processing personal data of individuals.
関連するEUの法的枠組みはGDPRである。コネクテッドビークルに関係して行われるデータの取扱いに個人データの取扱いが含まれる一切の場合にGDPRが適用される。

10. Additionally to the GDPR, directive 2002/58/EC as revised by 2009/136/EC (hereinafter - "ePrivacy directive"),**sets a specific standard for all actors that wish to store or access information stored in the terminal equipment of a subscriber or user in the European Economic Area (EEA).**
GDPRに加え、2009/136/ECにより改訂された指令2002/58/EC（以下「eプライバシー指令」）は、**欧州経済領域（EEA）内に存在する加入者又はユーザーの端末機器に**

[10] Data protection aspects of using connected and non-connected vehicles; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.
「コネクテッドビークル及び非コネクテッドビークルの使用に伴うデータ保護側面」、https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.
[11] Principles of cyber security for connected and automated vehicles; https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles.
「コネクテッドビークル及び自動運転車のサイバーセキュリティ原則」、https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles.
[12] Compliance package for a responsible use of data in connected cars; https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.
「コネクテッドカーにおけるデータの責任ある使用のための遵守パッケージ」、https://www.cnil.fr/en/connected- vehicles-compliance-package-responsible-use-data.

情報を保存したいか又は端末機器に保存された情報にアクセスしたいと考えるあらゆる行為主体を対象に特定の基準を規定している。

11. Indeed, if most of the ePrivacy directive provisions (art. 6, art. 9, etc.) only apply to providers of publicly available electronic communication services and providers of public communication networks, art. 5(3) ePrivacy directive is a general provision. It does not only apply to electronic communication services but also to every entity, private or public, that places on or reads information from a terminal equipment without regard to the nature of the data being stored or accessed.
実際、eプライバシー指令の規定の多く（第6条、第9条など）が公衆に利用可能な電子通信サービスのプロバイダー及び公衆通信ネットワークのプロバイダーにのみ適用されるとすれば、eプライバシー指令第5条(3)は一般規定である。本規定は、電子通信サービスのみならず、保存又はアクセスされるデータの性質に関係なく、端末機器に情報を保存するか又は端末機器から情報を読み取るあらゆる主体に、民間又は公的主体にかかわらず、適用される。

12. Regarding the notion of *"terminal equipment"*, the definition is given by directive 2008/63/CE[13]. Art. 1 (a) defines the terminal equipment as an *"equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment"*.
「*端末機器*」という概念は指令2008/63/CEにより定義されている[13]。同指令第1条(a)は、端末機器を「*情報を送信し、取扱い、又は受信するために公衆情報通信ネットワークのインターフェースに直接又は間接的に接続された機器。（直接又は間接の）いずれの場合も、接続は有線、光ファイバーにより又は電磁的に行われうる。機器が端末と、ネットワークのインターフェースとの間に配置されている場合、当該接続は間接的である。(b）衛星通信地球局の設備*」であると定義する。

13. As a result, provided that the aforementioned criteria are met, the connected vehicle and device connected to it should be considered as a *"terminal equipment"*(just like a computer, a smartphone or a smart TV) and provisions of art. 5(3) ePrivacy directive apply where relevant.
結果として、前述の基準が満たされていれば、コネクテッドビークルとそれに接続されているデバイスは（コンピューター、スマートフォン、スマートテレビと全く同様に）「端末機器」であるとみなされ、該当する場合には、eプライバシー指令第5条(3)の規定が適用される。

14. As outlined by the EDPB in its opinion 5/2019 on the interplay between the ePrivacy directive and the GDPR[14], art. 5(3) ePrivacy directive provides that, as a rule, and subject to the exceptions to that rule mentioned in paragraph 17 below, prior consent is required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user. To the extent that the information stored in the end-user's device constitutes personal data, art. 5(3) ePrivacy directive shall take precedence over art. 6 GDPR with regards to the activity of storing or gaining access to this information[15]. Any processing operations of personal data following the aforementioned

[13] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version) (Text with EEA relevance); https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008L0063.
「情報通信端末機器市場における競争に関する2008年6月20日の委員会指令2008/63/EC」（法典化版）（EEA関連条文）、https://eur-lex.europa.eu/legal- content/EN/ALL/?uri=CELEX%3A32008L0063.

processing operations, including processing personal data obtained by accessing information in the terminal equipment, must have a legal basis under art. 6 GDPR in order to be lawful[16].

eプライバシー指令とGDPRとの相互作用に関する意見05/2019[14]の中でEDPBが概説するように、eプライバシー指令第5条(3)は、原則として、また以下のパラグラフ17で説明しているような原則に対する例外は存在するものの、加入者又はユーザーの端末機器に情報を保存するため又は端末機器に既に保存されている情報へのアクセスを取得するためには事前の同意を要件とすることを規定している。エンドユーザーのデバイスに保存されている情報が個人データを構成する限り、当該情報の保存又は当該情報へのアクセスの取得活動にはeプライバシー指令第5条(3)がGDPR第6条に優先して適用される[15]。端末機器の情報にアクセスすることにより取得される個人データの取扱いを含む、前述の取扱業務に続く個人データの取扱業務が適法であるためには、GDPR第6条に基づく法的根拠を備えなければならない[16]。

15. Since the controller, when seeking consent for the storing or gaining of access to information pursuant to art. 5(3) ePrivacy directive, will have to inform the data subject about all the purposes of the processing – including any processing following the aforementioned operations (meaning the "subsequent processing") – consent under art. 6 GDPR will generally be the most adequate legal basis to cover the processing of personal data following such operations (as far as the purpose of the following processing is comprehended by the data subject's consent, see paragraphs 53-54 below). Hence, consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the subsequent processing of personal data[17]. Indeed, when assessing compliance with art. 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection[18]. Moreover, controllers must take into account the impact on data subjects' rights when identifying the appropriate lawful basis in order to respect the principle of fairness[19]. The bottom line is that art. 6 GDPR cannot be relied upon by controllers in order to lower the additional protection provided by art. 5(3) ePrivacy directive.

管理者は、eプライバシー指令第5条(3)に基づき情報の保存又は情報へのアクセス取得作業のための同意を求める場合、当該作業に続く一切の取扱い（つまり「その後の取扱い」）を含む、あらゆる取扱いの目的についてデータ主体に通知する必要があるため、GDPR第6条の同意が、一般に、当該作業に続くその後の個人データの取扱いを含めるためのもっとも適切な法的根拠となるであろう（その後の取扱いの目的が当該データ主体の同意に含まれる場合。以下のパラグラフ53及び54を参照のこと）。したがって、同意は、情報の保存及び既に保存されている情報へのアクセスの取得、並びにその後の個人データの取扱いの両方の法的根拠となる可能性が高い[17]。実際、GDPR第6条への遵守を評価する際は、取扱いが、全体として見た場

[14] European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019 (hereinafter - "Opinion 5/2019"), paragraph 40.
欧州データ保護会議（EDPB）、「eプライバシー指令とGDPRの相互作用に関する、特にデータ保護当局の職務権限、職務及び権限に関する意見05/2019」、2019年3月12日採択（以下「意見05/2019」）、パラグラフ40。

[15] Ibid, paragraph 40.
前掲パラグラフ40。

[16] Ibid, paragraph 41.
前掲パラグラフ41。

[17] Consent required by art. 5(3) of the "ePrivacy" directive and consent needed as a legal basis for the processing of data (art. 6 GDPR) for the same specific purpose can be collected at the same time (for example, by checking a box clearly indicating what the data subject is consenting to).

合に、EU議会が追加的保護を与えようとした特定の活動を伴うものであるかどうかを考慮すべきである[18]。さらに、管理者は、公正性の原則を尊重するため、適切な法的根拠を明らかにする際にはデータ主体の権利に与える影響を考慮しなければならない[19]。結論としては、eプライバシー指令第5条(3)に規定される追加的保護を引き下げるために管理者がGDPR第6条を取扱いの根拠法令とすることはできないということである。

16. The EDPB recalls that the notion of consent in the ePrivacy directive remains the notion of consent in the GDPR and must meet all the requirements of the consent as provided by art. 4(11) and 7 GDPR.
EDPBは、eプライバシー指令の同意の概念がGDPRの同意の概念を維持し、GDPR第4条(11)及び第7条により規定されている同意に関するあらゆる要件を満たさなければならないことを想起する。

17. However, while consent is the principle, art. 5(3) ePrivacy directive allows the storing of information or the gaining of access to information that is already stored in the terminal equipment to be exempted from the requirement of informed consent, if it satisfies one of the following criteria:
しかしながら、同意を得ることが原則ではあるものの、eプライバシー指令第5条(3)では、端末機器への情報の保存又は端末機器に既に保存されている情報へのアクセスの取得について、当該行為が次のいずれかの基準を満たす場合は、説明を受けた上での同意の要件の適用除外を認めている。

- ☐ **Exemption 1:** for the sole purpose of carrying out the transmission of a communication over an electronic communications network;
- ☐ **適用除外1:** 電子通信ネットワークを介した通信の送信を実行することのみを目的とする場合、

- ☐ **Exemption 2:** when it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.
- ☐ **適用除外2:** 加入者又はユーザーから明確に要求された情報社会サービスのプロバイダーが当該サービスを提供するために厳密に必要である場合。

18. In such cases, the processing of personal data including personal data obtained by accessing information in the terminal equipment is based on one of the legal bases as provided by art. 6 GDPR. For example, consent is not needed when data processing is necessary to provide GPS navigation services requested by the data subject when such services can be qualified as information society services.
このような場合、端末機器の情報にアクセスすることにより取得される個人データを含む個人データの取扱いは、GDPR第6条に規定される法的根拠の一つに基づき実施されるものとなる。例えば、データ主体による要求に応じてGPSナビゲーション・サービスを提供するためにデータを取扱う必要性がある場合、当該サービスを

「eプライバシー」指令第5条(3)により要求される同意と、同一の特定目的のためのデータの取扱いの法的根拠として必要とされる同意（GDPR第6条）とは（例えばデータ主体が同意しようとしている内容を明確に示すボックスにチェックを入れることにより）同時に取得することができる。

[18] Opinion 5/2019, paragraph 41.
「意見05/2019」、パラグラフ41。

[19] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, paragraph 1.
欧州データ保護会議(EDPB)、「データ主体へのオンラインサービスの提供に関連するGDPR第6条(1)(b)に基づく個人データの取扱いに関するガイドライン02/2019」、バージョン2.0、2019年10月8日、パラグラフ1。

情報社会サービスとみなすことが可能であれば同意を得る必要はない。

1.3 Scope
範囲

19. The EDPB would like to point out that these guidelines are intended to facilitate compliance of the processing of personal data carried out by a wide range of stakeholders working in this environment. However, they are not intended to cover all use cases possible in this context or to provide guidance for every possible specific situation.
EDPBは、このような環境に従事する幅広いステークホルダーが個人データを取扱う際、法令に従ったものとなるよう手助けすることが本ガイドラインの意図しているところである点を指摘したい。しかしながら、こうした文脈でのあらゆる使用例を網羅することも、可能性のあるあらゆる特定の状況に対する指針を示すことも本ガイドラインの意図ではない。

20. The scope of this document focuses in particular on the personal data processing in relation to the non-professional use of connected vehicles by data subjects: e.g., drivers, passengers, vehicle owners, other road users, etc. More specifically, it deals with the personal data:
本ガイドラインでは、その適用範囲として、特にデータ主体、例えば運転者、同乗者、車両の所有者、その他の道路利用者等によるコネクテッドビークルの業務外での使用に関連する個人データの取扱いに焦点をあてている。より具体的に言えば、本ガイドラインでは次の個人データを取扱う。
(i) processed inside the vehicle, (ii) exchanged between the vehicle and personal devices connected to it (e.g., the user's smartphone) or (iii) collected locally in the vehicle and exported to external entities (e.g., vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.
(i)車両内で取扱われるもの、(ii)車両と車両に接続された個人用デバイス（例えばユーザーのスマートフォン）との間で交換されるもの、又は(iii)車両内で収集され、追加的取扱いのために外部にある事業体（例えば自動車メーカー、インフラの管理者、保険会社、自動車の修理業者）に出力されるもの、である。

21. The connected vehicle definition has to be understood as a broad concept in this document. It can be defined as a vehicle equipped with many electronic control units (ECU) that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle. As such, data can be exchanged between the vehicle and personal devices connected to it, for instance allowing the mirroring of mobile applications to the car's in-dash information and entertainment unit. Also, the development of standalone mobile applications, meaning independent of the vehicle (for example, relying on the sole use of the smart phone) to assist drivers is included in the scope of this document since they contribute to the vehicle's connectivity capacities even though they may not effectively rely on the transmission of data with the vehicle *per se*. Applications for connected vehicles are multiple and diverse and can include[20]:
本ガイドラインで定義されるコネクテッドビークルは広い概念であることを理解しなければならない。コネクテッドビークルは、車両内外の他のデバイスとの情報共有を可能にする車両内ネットワーク及び接続機能を通じて相互につながる、多数の電子制御装置（ECU）を搭載した車両であると定義できる。このため、車両と車両に接続された個人用デバイスとの間でデータを交換でき、例えば、モバイルアプリケーションを車のダッシュボード内にある情報及びエンターテインメント装置にミラーリングすることができる。また、運転手を支援するための独立した、つまり車両から独立しているモバイルアプリケーション（例えばスマートフォンだけで使用するアプリケーション）の展開は、当該独立アプリケーションは実質的に車両自体とのデータの移転をしていないものの車両の接続能力に寄与しているため、本ガイ

ドラインの適用範囲に含まれる。コネクテッドビークルの用途は多様であり、次のものが含まれうる[20]。

22. *Mobility management:* functions that allow drivers to reach a destination quickly, and in a cost-efficient manner, by providing timely information about GPS navigation, potentially dangerous environmental conditions (e.g., icy roads), traffic congestion or road construction work, parking lot or garage assistance, optimized fuel consumption or road pricing.
移動管理： GPSナビゲーション、潜在的に危険な環境条件（例えば凍結した路面）、交通渋滞若しくは道路建設工事、駐車場若しくは自動車修理工場に関する支援、最適化された燃費、又は通行料金に関する適時な情報を提供することにより、運転者が迅速かつ費用効率の高い方法で目的地に到達することを可能にする機能。

23. *Vehicle management:* functions that are supposed to aid drivers in reducing operating costs and improving ease of use, such as notification of vehicle condition and service reminders, transfer of usage data (e.g., for vehicle repair services), customized "Pay As/How You Drive" insurances, remote operations (e.g., heating system) or profile configurations (e.g., seat position).
車両管理： 車両の状態の通知や保守点検に関するリマインダー、（例えば自動車修理サービスのための）使用状況データの移転、運転者一人ひとりに合わせた「走行距離連動型／運転行動連動型」の保険、（例えば暖房システムの）リモート操作又は（例えばシート位置などの）プロファイル設定など、運転者にとっての運用コストを引下げ、使い勝手を向上させるのに役立つと思われる機能。

24. *Road safety:* functions that warn the driver of external hazards and internal responses, such as collision protection, hazard warnings, lane departure warnings, driver drowsiness detection, emergency call (eCall) or crash investigation "black-boxes" (event data recorder).
交通安全： 衝突保護、ハザード警告、車線逸脱警報、運転者の眠気検知、緊急通報（eCall）、又は衝突調査「ブラックボックス」（事故データレコーダー）など、外部の危険及び運転者の反応に関して運転者に警告する機能。

25. *Entertainment :* functions providing information to and involving the entertainment of the driver and passengers, such as smart phone interfaces (hands free phone calls, voice generated text messages), WLAN hot spots, music, video, Internet, social media, mobile office or "smart home" services.
娯楽： スマートフォン・インターフェース（ハンズフリー通話、音声合成テキストメッセージ）、WLANホットスポット、音楽、ビデオ、インターネット、ソーシャルメディア、モバイルオフィス、又は「スマートホーム」サービスなど、運転者と同乗者に情報及び娯楽を提供する機能。

26. *Driver assistance :* functions involving partially or fully automated driving, such as operational assistance or autopilot in heavy traffic, in parking, or on highways,
運転支援： 交通渋滞時、駐車時、又は高速道路における運転支援又はオートパイロットなど、部分的又は完全に自動化された運転を伴う機能。

27. *Well-being :* functions monitoring the driver's comfort, ability and fitness to drive such as fatigue detection or medical assistance.
健康状態： 疲労検知や医療支援など、運転者にとっての快適さ、運転するための

[20] PwC Strategy 2014. "In the fast lane. The bright future of connected cars": https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.
「PwC戦略2014」。「高速走行中。コネクテッドカーの明るい未来」。 https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.

能力及び適性を監視する機能。

28. Hence, vehicles can be natively connected or not and personal data can be collected through several means, including: (i) vehicle sensors, (ii) telematics boxes or (iii) mobile applications (e.g. accessed from a device belonging to a driver). In order to fall within the scope of this document, mobile applications need to be related to the environment of driving. For example, GPS navigation applications are in-scope. Applications whose functionalities only suggest places of interest (restaurants, historic monument, etc.) to drivers fall, however, outside the scope of these guidelines.
したがって、車両はそれ自体を接続させることもさせないこともでき、個人データの収集は、次のものを含む幾つかの手段で行うことができる。（i）車両センサー、(ii)テレマティクス・ボックス、又は(iii)（例えば運転者が所有するデバイスからアクセスする）モバイルアプリケーション。本ガイドラインの適用範囲に該当するには、モバイルアプリケーションが運転環境に関連するものである必要がある。例えば、GPSナビゲーション・アプリケーションは適用範囲内である。しかしながら、運転者にとって関心のある場所（レストラン、歴史的建造物など）を提案する機能のみのアプリケーションは、本ガイドラインの適用範囲外である。

29. Much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data. For instance, data include directly identifiable data (e.g., the driver's complete identity), as well as indirectly identifiable data such as the details of journeys made, the vehicle usage data (e.g., data relating to driving style or the distance covered), or the vehicle's technical data (e.g., data relating to the wear and tear on vehicle parts), which, by cross-referencing with other files and especially the vehicle identification number (VIN), can be related to a natural person. Personal data in connected vehicles can also include metadata, such as vehicle maintenance status. In other words, any data that can be associated with a natural person therefore fall into the scope of this document.
コネクテッドビークルにより生成されるデータの多くは、識別された自然人又は識別可能な自然人に関連するものであり、したがって個人データを構成する。例えば、これらのデータには、直接識別可能なデータ（例えば運転者の完全な身元情報）に加え、走行ルートの詳細、車両の使用状況データ（例えば運転スタイルや走行距離に関連するデータ）又は車両の技術データ（例えば車両部品の摩耗に関するデータ）などの間接的に識別可能なデータが含まれうる。間接的なデータは、他の記録、特に車両識別番号（VIN）と相互参照することにより、ある自然人に関連付けることができる。また、コネクテッドビークルの個人データには、車両のメンテナンス状況などのメタデータが含まれうる。つまり、自然人に関連付けることができるデータであれば、いずれも本ガイドラインの適用範囲に含まれる。

30. The connected vehicle ecosystem covers a wide spectrum of stakeholders. This ecosystem more precisely includes traditional actors of the automotive industry as well as emerging players from the digital industry. Hence, these guidelines are directed towards vehicle manufacturers, equipment manufacturers and automotive suppliers, car repairers, automobile dealerships, vehicle service providers, fleet managers, motor insurance companies, entertainment providers, telecommunication operators, road infrastructure managers and public authorities as well as data subjects. The EDPB underlines that the categories of data subjects will differ from one service to another (e.g., drivers, owners, passengers, etc.). This is a non-exhaustive list as the ecosystem entails a wide variety of services, including services for which a direct authentication or identification is needed and services for which this is not needed.
コネクテッドビークルのエコシステムは、幅広いステークホルダーを対象としている。正確に言えば、自動車業界の従来の参加者のみならず、デジタル業界の新たな

参加者も当該エコシステムに含まれる。したがって、本ガイドラインは、自動車メーカー、機器メーカー、自動車部品供給業者、自動車修理業者、自動車販売業者、自動車関連サービスのプロバイダー、フリート管理者、自動車保険会社、エンターテインメントプロバイダー、情報通信事業者、道路インフラの管理者、公的機関、及びデータ主体を対象とする。EDPBは、データ主体の類型が（例えば運転者、所有者、同乗者など）サービスごとに異なる点を強調する。エコシステムには、直接的な認証又は識別を行う必要があるサービス及びそうする必要のないサービスなど、多様なサービスが含まれるため、前述の列挙は全体を網羅したものではない。

31. Some data processing performed by natural persons within the vehicle fall within *"the course of a purely personal or household activity"* and are consequently out of the scope of the GDPR[21]. In particular, this concerns the use of personal data within the vehicles by the sole data subjects who provided such data into the vehicle's dashboard. However, the EDPB recalls that according to its recital 18 the GDPR *"applies to controllers or processors which provide the means for processing personal data for such personal or household activities"*.
自然人により車両内で実行されるデータ取扱いの一部は、「*純粋に私的な行為又は家庭内の行為の過程*」に含まれ、その結果、GDPRの適用範囲外になる[21]。特に、データ主体単独で、車両のダッシュボードにデータを入力するような車両内における個人データの使用がこれに該当する。しかしながら、EDPBは、GDPR前文第18項に従い、GDPRが「*そのような私的な行為又は家庭内の行為のために個人データの取扱いの手段を提供する管理者又は処理者に対して適用される*」点を想起する。

1.3.1 Out of scope of this document
本ガイドラインの適用範囲外となるもの

32. Employers providing company cars to members of their staff might want to monitor their employee's actions (e.g., in order to ensure the safety of the employee, goods or vehicles, to allocate resources, to track and bill a service or to check working time). Data processing carried out by employers in this context raises specific considerations to the employment context, which might be regulated by labour laws at the national level that cannot be detailed in these guidelines[22].
従業員に社用車を提供する使用者が（例えば従業者、商品若しくは車両の安全を確保する目的で、リソースを割り当てる目的で、サービスを追跡し、これに課金する目的で、又は労働時間を確認する目的で）従業者の行動を監視したい場合がある。このような監視の目的での使用者により行われるデータの取扱いは、雇用の観点から問題を提起する。当該問題は国内の労働法による規制対象となると考えられ、本ガイドラインで詳しく説明することはできない[22]。

33. While the data processing in the context of commercial vehicles used for professional purposes (such as public transport) and shared transport and MaaS solution may raise specific considerations which fall out of the scope of these general guidelines, many of the principles and recommendations set out here will also be applicable to those types of processing.
（公共交通機関などの）業務目的、並びに乗合輸送及びMaaS（Mobility as a Service）輸送に利用される商用車に関係するデータの取扱いからも考慮すべき特別な問題が生じうるが、本ガイドラインの対象外である。しかしながら、当該商用車関連の取

[21] See GDPR, Article 2(2)(c).
GDPR第2条(2)(c)を参照のこと。
[22] The Article 29 Working Party elaborated on this in its WP249 Opinion 2/2017 on data processing at work; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.
第29条作業部会は、同作業部会の「職場におけるデータの取扱いに関する意見02/2017」で本件に関して詳しく説明している。https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

扱いについても、本ガイドラインで定める原則及び勧告の多くを適用することが可能であろう。

34. Connected vehicles being radio-enabled systems, they are subject to passive tracking such as Wi-Fi or Bluetooth tracking. In that sense they do not differ from other connected devices and fall in the scope of the ePrivacy directive which is currently being revised. This therefore excludes also large-scale tracking of Wi-Fi equipped vehicles[23] by a dense network of bystanders who use common smartphone location services. These routinely report all visible Wi-Fi networks to central servers. Since built-in Wi-Fi can be considered a secondary vehicle identifier[24], this risks a systematic ongoing collection of complete vehicle movement profiles.
コネクテッドビークルは無線対応システムであるため、Wi-Fi又はBluetoothトラッキングなどのパッシブ方式の追跡の対象となる。その意味においてコネクテッドビークルは他の接続装置と異ならず、現在改訂が進められているeプライバシー指令の適用範囲には含まれていない。従って、付近にいて一般的なスマートフォンの位置情報サービスを利用している人々によって作り出される密集したネットワークによるWi-Fi搭載車両[23]の大規模追跡についても対象外とする。当該位置情報サービスは、認識可能なあらゆるWi-Fiネットワークを中央サーバーに定期的に報告する。内蔵Wi-Fiは二次的な車両識別子とみなすことができるため[24]、これにより、車両の完全な移動プロファイルの体系的かつ継続的な収集が行われる危険性がある。

35. Vehicles are increasingly equipped with image recording devices (e.g., car parking camera systems or dashcams). Since this deals with the issue of filming public places, which requires an assessment of the relevant legislative framework which is specific to each Member State, this data processing is out of the scope of these guidelines.
録画装置（駐車支援カメラ・システム又はドライブレコーダーなど）を装備する車両が増えている。このような録画行為は公共空間の撮影という問題を伴い、各加盟国固有の関連法令枠組みを評価する必要があるため、このようなデータの取扱いは本ガイドラインの適用範囲外である。

36. The processing of data enabling Cooperative Intelligent Transport Systems (C-ITS) – as defined in the directive 2010/40/EU[25] has been dealt with in a specific opinion by the Article 29 Working Party[26]. While the definition of the C-ITS concept in the directive does not bear any technical specifications, the Article 29 Working Party focuses in its opinion on short-range communications, i.e. that do not involve the intervention of a network operator. More specifically, it provides analysis for specific use cases built for initial deployment and committed to assess at a later stage the new issues that will be undoubtedly raised when higher level of automation will be implemented. Since the data protection implications in the context of C-ITS are very specific (unprecedented amounts of location data, continuous broadcasting of personal data, exchange of data between vehicles and other road infrastructural facilities, etc.) and that it is still being discussed at the European level, the processing of personal data in that context is not covered by these guidelines.

[23] See for details: https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically- Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html.
詳細に関しては以下を参照のこと。https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically- Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html.

[24] Markus Ullmann, Tobias Franz, and Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, p. 32-37.
Markus Ullmann、Tobias Franz及びGerd Nolden、「二次的車両識別子に基づく車両の識別 --分析及び測定」、講演要旨集、VEHICULAR 2017年、車両システム、技術及びアプリケーションの進歩に関する第6回国際会議、フランス、ニース、2017年7月23日から27日まで、32-37頁。

指令2010/40/EU[25]で定義されているような協調型高度道路交通システム（C-ITS）を可能にするデータの取扱いは、この問題に絞った第29条作業部会意見で扱っている[26]。同指令におけるC-ITSの概念の定義には技術仕様が含まれていないものの、第29条作業部会は、短距離通信、つまりネットワーク事業者の介入を伴わない通信に焦点をあてている。より具体的に言えば、同作業部会では、より高度な自動システムが導入される際に間違いなく提起される新たな問題に関しては、その段階で評価することを明言した上で、初期のシステムに基づく使用例の分析結果を示している。C-ITSの関係におけるデータ保護の特徴は（前例のない量の位置データ、個人データの継続的な発信、車両と他の道路インフラ施設とのデータ交換など）極めて特殊であり、欧州レベルではまだ議論されている段階にあるため、C-ITSに関係する個人データの取扱いは本ガイドラインの対象外とする。

37. Finally, this document does not aim to address all possible issues and questions raised by connected vehicles and can therefore not be considered as exhaustive.
最後に、本ガイドラインは、コネクテッドビークルに関連して生ずる可能性のあるあらゆる問題及び疑問点に対処することをねらいとするものではないため、本ガイドラインにおいて全ての問題が網羅されているとはみなすことはできない。

1.4 Definitions
定義

38. The **processing** of personal data encompasses any operation that involves personal data such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, etc[27].
個人データの**取扱い**には、収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布又はそれら以外に利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊のような、個人データが関与する業務遂行が含まれる[27]。

39. The **data subject** is the natural person to whom the data covered by the processing relate. In the context of connected vehicles, it can, in particular, be the driver (main or occasional), the passenger, or the owner of the vehicle[28].
データ主体は、取扱いの対象となるデータが関係する自然人である。コネクテッドビークルの場合、当該自然人として、特に運転者（その車両を主に運転している者と臨時で運転する者）、同乗者、又は車両の所有者が考えられる[28]。

40. The **data controller** is the person who determines the purposes and means of processing that take place in connected vehicles[29]. Data controllers can include service providers that

[25] Directive 2010/40/EU of 7 July 2020 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040.
「道路輸送分野における高度道路交通システムの配備及び他の輸送モードとのインターフェースのための枠組みに関する2020年7月7日の指令2010/40/EU」、https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040.
[26] Article 29 Working Party - Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS); http://ec.europa.eu/newsroom/article29/item- detail.cfm?item_id=610171.
第29条作業部会、「協調型高度道路交通システム（C-ITS）との関係における個人データの取扱いに関する意見03/2017」、http://ec.europa.eu/newsroom/article29/item- detail.cfm?item_id=610171.
[27] See GDPR, Article 4 (2).
GDPR第4条(2)を参照のこと。
[28] See GDPR, Article 4 (1).
GDPR第4条(1)を参照のこと。

process vehicle data to send the driver traffic-information, eco-driving messages or alerts regarding the functioning of the vehicle, insurance companies offering *"Pay As You Drive"* contracts, or vehicle manufacturers gathering data on the wear and tear affecting the vehicle's parts to improve its quality. Pursuant to art. 26 GDPR, two or more controllers can jointly determine the purposes and means of the processing and thus be considered as joint controllers. In this case, they have to clearly define their respective obligations, especially as regards the exercising of the rights of data subjects and the provision of information as referred to in art. 13 and 14 GDPR.

データ管理者は、コネクテッドビークルに関連して行われる取扱いの目的及び手段を決定する者である[29]。データ管理者には、交通情報、エコドライブメッセージ又は車両の機能に関する警告を運転者に送信するために車両データを取扱うサービスプロバイダー、利用ベース型の契約を提供する保険会社、又は車両の品質を向上させるために車両部品に影響を及ぼす摩耗に関するデータを収集する自動車メーカーを含めることができる。GDPR第26条に従い、二者以上の管理者が共同して取扱いの目的及び方法を決定することが可能であり、このとき共同管理者とみなされる。この場合、共同管理者は、とりわけ、データ主体の権利の行使に関する義務、並びに、第13 条及び第14 条に規定する情報を提供すべき管理者それぞれの義務を明瞭に定める必要がある。

41. The **data processor** is any person who processes personal data for and on behalf of the data controller[30]. The data processor collects and processes data on instruction from the data controller, without using those data for its own purposes. As an example, in a number of cases, equipment manufacturers and automotive suppliers may process data on behalf of vehicle manufacturers (which does not imply they cannot be a data controller for other purposes). In addition to requiring data processors to implement appropriate technical and organizational measures in order to guarantee a security level that is adapted to risk, art. 28 GDPR sets out data processors' obligations.

データ処理者とは、データ管理者のためかつデータ管理者の代わりに個人データを取扱う者である[30]。データ処理者は、データ管理者の指示に基づいてデータを収集し取扱い、そうしたデータを独自の目的で利用することはない。一例として、機器メーカーと自動車部品メーカーが自動車メーカーの代わりにデータを取扱う（これは、前二者が他の目的の関係においてデータ管理者になり得ないことを意味するものではない）ケースも多い。GDPR第28条は、データ処理者に対し、リスクに相応する水準の安全管理の実施を保証するための適切な技術上及び組織上の保護措置を実装することを要求しており、それ以外にもデータ処理者の複数の義務を規定する。

42. The **recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not[31]. As an example, a commercial partner of the service provider that receives from the service provider personal data generated from the vehicle is a recipient of personal data. Whether they act as a new data controller or as a data processor, they shall comply with all the obligations imposed by the GDPR.

取得者とは、第三者であるか否かを問わず、個人データの開示を受ける自然人若

[29] See GDPR, Article 4 (7) and the European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (hereinafter - "Guidelines 07/2020").
GDPR第4条(7)及びEDPB、「GDPRにおける管理者及び処理者の概念に関するガイドライン07/2020」（以下「ガイドライン07/2020」）を参照のこと。
[30] See GDPR, Article 4 (8) and the Guidelines 07/2020.
GDPR第4条(8)及び「ガイドライン07/2020」を参照のこと。

しくは法人、公的機関、部局又はその他の組織を意味する[31]。一例として、車両から生成される個人データをサービスプロバイダーから受け取る当該サービスプロバイダーの商業的なパートナーは個人データの取得者である。当該パートナーは、新規のデータ管理者として行為する場合も、データ処理者として行為する場合も、GDPRにより課せられるあらゆる義務を遵守する。

43. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients[32]; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. As an example, law enforcement authorities are authorized third parties when they request personal data as part of an investigation in accordance with European Union or Member State law.
ただし、EU法又は加盟国の国内法に従って特別の調査の枠組み内で個人データを取得できる公的機関は、取得者とはみなされない[32]。公的機関による当該データの取扱いは、その取扱いの目的に従い、適用されるデータ保護の規定を遵守するものとする。一例として、法執行機関がEU法又は加盟国の国内法に従った調査の一環として個人データを要求する場合、当該機関は取扱い権限のある第三者となる。

1.5 Privacy and data protection risks
プライバシー及びデータ保護に対するリスク

44. Article 29 Working Party has already expressed several concerns about Internet of Things (IoT) systems that can also apply to connected vehicles[33]. The issues relating to data security and control already stressed regarding IoT are even more sensitive in the context of connected vehicles, since it entails road safety concerns – and can impact the physical integrity of the driver – in an environment traditionally perceived as isolated and protected from external interferences.
第29条作業部会はモノのインターネット（IoT）システムに関する懸念を既に表明しており、その幾つかはコネクテッドビークルにもあてはまりうる[33]。IoTに関して既に強調されているデータの安全性及び管理上の問題は、コネクテッドビークルとの関係ではさらにセンシティブである。これは、コネクテッドビークルの場合、従来であれば外部の干渉から隔離されかつ保護されているとみなされていた環境の中で、交通安全の問題を伴い、かつ運転者の身体的な完全性に影響を与えるかねないからである。

45. Also, connected vehicles raises significant data protection and privacy concerns regarding the processing of location data as its increasingly intrusive nature can put a strain on the current possibilities to remain anonymous. The EDPB wants to place particular emphasis and raise stakeholders' awareness to the fact that the use of location technologies requires the implementation of specific safeguards in order to prevent surveillance of individuals and misuse of the data.
また、コネクテッドビークルの位置データの取扱いの侵害性が強まっており、現在の匿名性を保てる可能性を脅かしているため、重大なデータ保護及びプライバシー

[31] See GDPR, Article 4 (9) and the Guidelines 07/2020.
GDPR第4条(9)及び「ガイドライン07/2020」を参照のこと。
[32] GDPR, Article 4 (9) and Recital 31.
GDPRの第4条(9)及び前文第31項。
[33] Article 29 Working Party – Opinion 8/2014 on the Recent Developments on the Internet of Things; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.
第29条作業部会、「モノのインターネットの最近の進展に関する意見08/2014」、https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

上の懸念を生じている。EDPBは、個人の監視及びデータの不正使用を防ぐため、位置情報技術の使用には特別な保護措置の導入が必要であるという事実を特に強調し、この点に関するステークホルダーの認識を高めたい。

1.5.1 Lack of control and information asymmetry
管理の不足及び情報の非対称性

46. Vehicle drivers and passengers may not always be adequately informed about the processing of data taking place in or through a connected vehicle. The information may be given only to the vehicle owner, who may not be the driver, and may also not be provided in a timely fashion. Thus, there is a risk that there are insufficient functionalities or options offered to exercise the control necessary for affected individuals to avail themselves of their data protection and privacy rights. This point is of importance since, during their lifetime, vehicles may belong to more than one owner either because they are sold or because they are being leased rather than purchased.
コネクテッドビークル内又はコネクテッドビークルを介して行われるデータの取扱いに関し、車両の運転者及び同乗者が常に適切に説明を受けているとは限らない。当該情報が車両所有者にのみ提供され、その者が運転者ではない場合があり、また、情報が適時に提供されない場合もある。このため、影響を受ける個人がデータ保護及びプライバシーに関する権利を享受するために必要な管理権限を行使するのに十分な機能又は選択肢が提供されない危険性が存在する。この点は重要である。その理由は、転売されるか又は購入する代わりにリースされるなどの原因により、車両というものが、その耐用期間中に所有者が変わりうるためである。

47. Also, communication in the vehicle can be triggered automatically as well as by default, without the individual being aware of it. In the absence of the possibility to effectively control how the vehicle and its connected equipment interact, it is bound to become extraordinarily difficult for the user to control the flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function creep.
また、車両内の個人が気付かないまま、車両搭載の通信機能が自動で起動している場合、及び初期設定で起動している場合がある。車両とその接続機器が相互作用する方法を効果的に管理できる可能性がない場合、ユーザーがデータの流れを管理することは極めて困難にならざるを得ない。データのその後の使用を管理し、潜在的な目的外流用（ファンクション・クリープ）を防ぐことはなおさら困難であろう。

1.5.2 Quality of the user's consent
ユーザーの同意の質

48. The EDPB underlines that, when the data processing is based on consent, all elements of valid consent have to be met which means that consent shall be free, specific and informed and constitutes an unambiguous indication of the data subject's wishes as interpreted in EDPB guidelines on consent[34]. Data controllers need to pay careful attention to the modalities of obtaining valid consent from different participants, such as car owners or car users. Such consent must be provided separately, for specific purposes and may not be bundled with the contract to buy or lease a new car. Consent must be as easily withdrawn as it is given.
EDPBは、データの取扱いが同意に基づいて行われる場合に関し、有効な同意のあらゆる要素が満たされる必要がある点を強調する。これは、同意が、EDPBの同意に関するガイドラインの解釈に従い、自由になされ、特定されており、かつ説明を受けたものであり、また、不明瞭ではないデータ主体の意思の表示を構成するものであることを意味する[34]。データ管理者は、車の所有者及び車のユーザーなど、多

[34] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 4 May 2020 (hereinafter - "Guidelines 05/2020").

様な参加者から有効な同意を取得するあり方に注意を払う必要がある。そのような同意は、特定の目的ごとに個別に与えられたものでなければならず、また新車を購入又はリースする契約にまとめることはできない。同意は、与える場合と同程度に容易に撤回できなければならない。

49. The same has to be applied when consent is required to comply with the ePrivacy directive, for example if there is a storing of information or the gaining of access to information already stored in the vehicle as required in certain cases by art. 5(3) of the ePrivacy directive. Indeed, as outlined above, consent in this context has to be interpreted in light of the GDPR.
eプライバシー指令に適合するための同意を得る必要がある場合、例えば、eプライバシー指令第5条(3)に規定される特定のケースで要件とされるように、車両に情報を保存するか又は車両に既に保存されている情報へのアクセスを取得するため、同意を得る場合においても、同様のことがあてはまる。上記で概説したように、実際、このような場合の同意はGDPRに照らして解釈しなくてはならない。

50. In many cases, the user may not be aware of the data processing carried out in his/her vehicle. Such lack of information constitutes a significant barrier to demonstrating valid consent under the GDPR, as the consent must be informed. In such circumstances, consent cannot be relied upon as a legal basis for the corresponding data processing under the GDPR.
自己の車の中で行われているデータの取扱いにユーザーが気付いていないケースも多い。同意は説明を受けたものでなければならないため、このような情報の不足は、GDPRに基づく有効な同意であることの証明を妨げる重大な障壁となる。このような状況では、GDPRに基づく当該データの取扱いの法的根拠を同意に求めることはできない。

51. Classic mechanisms used to obtain individuals' consent may be difficult to apply in the context of connected vehicles, resulting in a "low-quality" consent based on a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals. In practice, consent might also be difficult to obtain for drivers and passengers who are not related to the vehicle's owner in the case of second-hand, leased, rented or borrowed vehicles.
コネクテッドビークルの場合には個人の同意を得るために利用されていた従来の仕組みをあてはめるのが難しい可能性があり、その結果、情報不足による「低品質」な同意になるか又は個人の選択に合わせて細かく調整した同意を得ることが事実上不可能な結果となる。現実問題として、中古車、リース車、レンタル車、借用車の場合も、車の所有者とは無関係な運転者及び同乗者の同意を得るのが難しい可能性がある。

52. When the ePrivacy directive does not require the data subject consent, the controller nonetheless has the responsibility of choosing the legal basis under art. 6 GDPR that is most appropriate to the case for the processing of personal data.
eプライバシー指令によりデータ主体の同意が要要とされない場合でも、管理者は、個人データの取扱い事例ごとに、GDPR第6条の最も適切な法的根拠を選択する責任を負う。

1.5.3 Further processing of personal data
個人データの追加的取扱い

53. When data is collected on the basis of consent as required by art. 5(3) of the ePrivacy directive or on one of the exemptions of art. 5(3), and subsequently processed in

EDPB、「規則2016/679に基づく同意に関するガイドライン05/2020」、バージョン1.1、2020年5月4日（以下「ガイドライン05/2020」）。

accordance with art. 6 GDPR, it can only be further processed either if the controller seeks additional consent for this other purpose or if the data controller can demonstrate that it is based on a Union or Member State law to safeguard the objectives referred to in art. 23 (1) GDPR[35]. The EDPB considers that further processing on the basis of a compatibility test according to art. 6(4) GDPR is not possible in such cases, since it would undermine the data protection standard of the ePrivacy directive. Indeed, consent, where required under the ePrivacy directive, needs to be specific and informed, meaning that data subjects must be aware of each data processing purpose and entitled to refuse specific ones[36]. Considering that further processing on the basis of a compatibility test according to art. 6(4) of the GDPR is possible would circumvent the very principle of the consent requirements set forth by the current directive.

eプライバシー指令第5条(3)の要件である同意又は同項の適用除外の一つに基づきデータが収集され、またその後の取扱いがGDPR第6条に従って実施される場合、当該データを追加的に取扱うことができるのは、管理者が当該他の目的の取扱いのための追加的同意を求めたか又は当該取扱いがGDPR第23条(1)に規定する対象を保護するためにEU法又は加盟国の国内法に基づいたものであることをデータ管理者が証明できる場合に限られる[35]。EDPBは、eプライバシー指令のデータ保護基準を低下させることになるため、そのような場合にはGDPR第6条(4)に規定する適合性基準に基づいた追加的取扱いを行うことはできないと考える。eプライバシー指令で要求される場合の同意は、実際、特定されかつ説明を受けたものでなければならない。つまり、データ主体はデータを取扱うそれぞれの目的を認識しており、個別に拒否する権利を有しなければならない[36]。GDPR第6条(4)に規定する適合性基準に基づいた追加的取扱いを行うことができると考えることは、現行指令に規定される同意要件の原則そのものを迂回することを意味するであろう。

54. The EDPB recalls that the initial consent will never legitimize further processing as consent needs to be informed and specific to be valid.

同意が有効であるためには説明を受け、特定されている必要があるため、EDPBは、最初の同意に基づき追加的取扱いが正当化されることは決してない点を想起する。

55. For instance, telemetry data, which is collected during use of the vehicle for maintenance purposes may not be disclosed to motor insurance companies without the users consent for the purpose of creating driver profiles to offer driving behaviour-based insurance policies.

例えば、メンテナンス目的で車両を使用する間に収集されたテレメトリデータを、ユーザーの同意なく、運転行動連動型保険契約を提供するために運転者のプロファイルを作成したいと考える自動車保険会社に開示してはならない。

56. Furthermore, data collected by connected vehicles may be processed by law enforcement authorities to detect speeding or other infractions if and when the specific conditions in the law enforcement directive are fulfilled. In this case, such data will be considered as relating to criminal convictions and offences under the conditions laid down by art. 10 GDPR and any applicable national legislation. Manufacturers may provide the law enforcement authorities with such data if the specific conditions for such processing are fulfilled. The EDPB points out that processing of personal data for the sole purpose of fulfilling requests made by law enforcement authorities does not constitute a specified, explicit and legitimate purpose within the meaning of art. 5(1)(b) GDPR. When law enforcement authorities are

[35] See also European Data Protection Board, Guidelines 10/2020 on restrictions under Article 23 GDPR.
また、EDPB、「GDPR第23条に基づく制限に関するガイドライン10/2020」も参照のこと。
[36] Guidelines 05/2020, sections 3.2 and 3.3.
「ガイドライン05/2020」、第3.2節及び第3.3節。

authorized by law, they could be third parties within the meaning of art. 4(10) GDPR, in this case manufacturers would be entitled to provide them with any data at their disposal subject to compliance with the relevant legal framework in each Member State.
さらに、コネクテッドビークルにより収集されるデータは、法執行指令の特定の条件が満たされる場合には、スピード違反及びその他の違反行為を検出する目的で法執行機関により取扱われうる。この場合、取扱うデータは、GDPR第10条及び該当の国内法により定められた条件に基づき有罪判決及び犯罪行為に関連する個人データとみなされる。当該取扱いのための特定の条件が満たされている場合、メーカーは該当データを法執行機関に提供することができる。EDPBは、法執行機関からの要求を充足することのみを目的とした個人データの取扱いがGDPR第5条(1)(b)の意味における特定され、明確であり、かつ、正当な目的を構成しない点を指摘する。法執行機関は、法律により取扱い権限がある場合、GDPR第4条(10)の意味における第三者に該当すると考えられる。その場合、メーカーは、加盟国ごとの関連する法的枠組みを遵守するため、自己の有するデータを法執行機関に提供する権利を有する。

1.5.4 Excessive data collection
データの過剰な収集

57. With the ever-increasing number of sensors being deployed in connected vehicles there is a very high risk of excessive data collection compared to what is necessary to achieve the purpose.
コネクテッドビークルに搭載されるセンサーの数が増え続けるのに伴い、目的を達成するために必要とされる範囲を超える、データの過剰な収集が行われるリスクが極めて高くなる。

58. The development of new functionalities and more specifically those based on machine learning algorithms may require a large amount of data collected over a long period of time.
新たな機能、より具体的には機械学習のアルゴリズムに基づく機能を開発するには、長期間にわたって収集される大量のデータが必要になりうる。

1.5.5 Security of personal data
個人データの安全管理

59. The plurality of functionalities, services and interfaces (e.g., web, USB, RFID, Wi-Fi) offered by connected vehicles increases the attack surface and thus the number of potential vulnerabilities through which personal data could be compromised. Unlike most IoT devices, connected vehicles are critical systems where a security breach may endanger the life of its users and people around. The importance of addressing the risk of hackers attempting to exploit connected vehicles' vulnerabilities is thus heightened.
コネクテッドビークルにより提供される機能、サービス及びインターフェース（Web、USB、RFID、Wi-Fiなど）が複数存在することは、ソフトウェアの攻撃対象領域を増やし、ひいては、個人データの漏えいを引き起こしかねない潜在的な脆弱性の数を増やすことになる。コネクテッドビークルは、大半のIoTデバイスとは異なり、危険度の高いシステムであり、安全管理違反によりユーザー及び周囲の人々の生命を危険にさらしかねない。このため、コネクテッドビークルの脆弱性を利用しようとするハッカーからのリスクに対処する重要性も大きい。

60. In addition, personal data stored on vehicles and/or at external locations (e.g., in cloud computing infrastructures) must be adequately secured against unauthorized access. For instance, during maintenance, a vehicle has to be handed to a technician who will require access to some of the vehicle's technical data. While the technician needs to have access to the technical data, there is a possibility that the technician could attempt to access all the data stored in the vehicle.

加えて、車両内及び／又は車外の場所（クラウド・コンピューティング・インフラなど）に保存されている個人データは、不正アクセスから適切に保護されなければならない。例えば、車両メンテナンス期間中、車両の技術データの一部へのアクセスを必要とする技術者に車両を引渡す必要がある。当該技術者は技術データにアクセスする必要がある一方で、車両に保存されている全データにアクセスしようと試みる可能性もある。

2 GENERAL RECOMMENDATIONS 一般勧告

61. In order to mitigate the risks for data subjects identified above, the following general recommendations should be followed by vehicle and equipment manufacturers, service providers or any other stakeholder who may act as data controller or data processor in relation to connected vehicles.
上記で明らかにされたデータ主体にとってのリスクを軽減するため、車両及び機器のメーカー、サービスプロバイダー、又はコネクテッドビークルに関連してデータ管理者若しくはデータ処理者として行為しうるその他のステークホルダーらは以下の一般勧告を遵守すべきである。

2.1 Categories of data データの種類

62. As noted in the introduction, most data associated with connected vehicles will be considered personal data to the extent that it is possible to link it to one or more identifiable individuals. This includes technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tire pressure). Certain data generated by connected vehicles may also warrant special attention given their sensitivity and/or potential impact on the rights and interests of data subjects. At present, the EDPB has identified three categories of personal data warranting special attention, by vehicle and equipment manufacturers, service providers and other data controllers: location data, biometric data (and any special category of data as defined in art. 9 GDPR) and data that could reveal offences or traffic violations.
冒頭で述べたように、コネクテッドビークルに関連する大半のデータは、一人以上の識別可能な個人に関連づけることができる範囲で個人データとみなされる。これには、車両の挙動（速度、走行距離など）に関する技術データ、及び車両の状態（エンジン冷却水の温度、エンジン回転数、タイヤの空気圧など）に関する技術データが含まれる。また、コネクテッドビークルにより生成される一部データは、その機微性及び／又はデータ主体の権利及び利益に対する潜在的な影響を考慮し、特別な注意を払う必要がありうる。EDPBは現在、車両及び機器のメーカー、サービスプロバイダー、並びにその他のデータ管理者により、特別な注意が払われる必要のある次の三つの種類の個人データを明らかにしている。すなわち、位置データ、生体データ（及びGDPR第9条で規定される特別な種類のデータ）、並びに犯罪行為及び交通違反を示す可能性のあるデータである。

2.1.1 Location data 位置データ

63. When collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should keep in mind that location data are particularly revealing of the life habits of data subjects. The journeys carried out are very characteristic in that they

enable one to infer the place of work and of residence, as well as a driver's centres of interest (leisure), and may possibly reveal sensitive information such as religion through the place of worship, or sexual orientation through the places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controller should be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing. As an example, when the processing consists in detecting the vehicle's movement, the gyroscope is sufficient to fulfil that function, without there being a need to collect location data.
個人データを収集する場合、車両及び機器のメーカー、サービスプロバイダー、並びにその他のデータ管理者は、位置データがデータ主体の生活習慣を特に露呈させる点に留意すべきである。走行ルートは、職場と住居の位置及び運転者の関心の中心（レジャー）を推定できるという点で極めて特徴的であり、また、参拝した場所を通じて信仰、又は訪問先を通じて性的指向などのセンシティブな情報を明らかにしうる。したがって、車両及び機器のメーカー、サービスプロバイダー、並びにその他のデータ管理者は、取扱いの目的に照らして、位置データを収集することが絶対に必要な場合を除き、当該データを収集しないよう特に注意するべきである。一例として、取扱いが車両の挙動の検出を目的とする場合、当該目的を達成するにはジャイロスコープ（角速度センサー）のデータを調べれば足り、位置データを収集する必要はない。

64. In general, collecting location data is also subject to compliance with the following principles:
一般に、位置データの収集は、次の原則に服する必要がある。

☐ adequate configuration of the frequency of access to, and of the level of detail of, location data collected relative to the purpose of processing. For example, a weather application should not be able to access the vehicle's location every second, even with the consent of the data subject;
- 取扱いの目的に照らした、収集される位置データへのアクセスの頻度とその詳細さの度合いの適切な設定。例えば、データ主体の同意があっても、車両の位置データに毎秒アクセスすることを気象アプリケーションに許可すべきではない。

☐ providing accurate information on the purpose of processing (e.g., is location history stored? If so, what is its purpose?);
- 取扱いの目的に関する正確な情報の提供（例えば位置データ履歴は保存されるか。保存されるなら、その目的は何か）。

☐ when the processing is based on consent, obtaining valid (free, specific and informed) consent that is distinct from the general conditions of sale or use, for example on the on-board computer;
- 取扱いが同意を根拠とする場合、例えば車載コンピューターに関する一般的な販売条件又は使用条件とは別に、有効な（自由になされ、特定され、かつ説明を受けた）同意を得ること。

☐ activating location only when the user launches a functionality that requires the vehicle's location to be known, and not by default and continuously when the car is started;
- 位置情報取得機能は、車両の位置を知る必要があるような機能をユーザーが起動した場合にのみ稼働させること。初期設定により車のエンジン始動時から継続的に稼働させない。

☐ informing the user that location has been activated, in particular by using icons (e.g., an arrow that moves across the screen);
- 特に（画面上を移動する矢印などの）アイコンを使い、位置情報取得機能が起動し

たことをユーザーに通知すること。

☐ the option to deactivate location at any time;
- いつでも位置情報取得機能を停止することができるようにすること。

☐ defining a limited storage period.
- 記録の保存期間を限定すること。

2.1.2 Biometric data
生体データ

65. In the context of connected vehicles, biometric data used for the purpose of uniquely identifying a natural person may be processed, within the remit of art. 9 GDPR and the national exceptions, among other things, to enable access to a vehicle, to authenticate the driver/owner, and/or to enable access to a driver's profile settings and preferences. When considering the use of biometric data, guaranteeing the data subject full control over his or her data involves, on the one hand, providing for the existence of a non-biometric alternative (e.g., using a physical key or a code) without additional constraint (that is, the use of biometrics should not be mandatory), and, on the other hand, storing and comparing the biometric template in encrypted form only on a local basis, with biometric data not being processed by an external reading/comparison terminal.
コネクテッドビークルにおいて、自然人を一意に識別する目的で利用される生体データは、特に車両へのアクセスを可能にし、運転者／所有者を認証し、及び／又は運転者のプロファイル設定と嗜好に関する情報へのアクセスを可能にする目的で、GDPR第9条の範囲内でかつ国内法の例外を除いて取扱われうる。生体データの使用を検討する場合、追加的な制約を加えることなく非生体認証による代替手段（例えば物理的な鍵又は暗号を使った方法）を用意する（つまり生体認証の使用を強制しない）一方で、生体認証テンプレートは暗号化し、車両内でのみ保存及び照合を行い、外部の読取り／照合端末機での生体データの取扱いを行わないことで、自己のデータを完全に管理できることをデータ主体に保証すること。

66. In the case of biometric data[37], it is important to ensure that the biometric authentication solution is sufficiently reliable, in particular by complying with the following principles:
生体データの場合[37]、特に次の原則を遵守することで、生体認証方式の十分な信頼性を確保することが重要である。

- the adjustment of the biometric solution used (e.g., the rate of false positives and false negatives) is adapted to the security level of the required access control;
- 必要とされるアクセス管理の安全性レベルに適合するように、利用する生体認証方式（例えば偽陽性率と偽陰性率）を調整すること。
- the biometric solution used is based on a sensor that is resistant to attacks (such as the use of a flat-printed print for fingerprint recognition);
- （指紋認識用に印刷したものを使用するなどの）攻撃に対する耐性を有するセンサーが採用された生体認証方式を利用すること。
- the number of authentication attempts is limited;
- 認証の試行回数を制限すること。
- the biometric template/model is stored in the vehicle, in an encrypted form using a cryptographic algorithm and key management that comply with the state of the art;

[37] The prohibition principle set out in article 9.1 GDPR only relates to "biometric data for the purpose of uniquely identifying a natural person".
GDPR第9条(1)に規定される禁止原則は、「自然人を一意に識別することを目的とする生体データ」にのみ関連するものである。

- 最新の技術水準の暗号化アルゴリズム及び暗号鍵管理を使い、生体認証テンプレート／モデルを暗号化された形式で車両に保存すること。
- the raw data used to make up the biometric template and for user authentication are processed in real time without ever being stored, even locally.
- 生体認証テンプレートを作成する際の生データ及びユーザー認証に利用される生データを、車両内にも保存せずにリアルタイムで取扱うこと。

2.1.3 Data revealing criminal offenses or other infractions
犯罪行為又はその他の違反行為を示すデータ

67. In order to process data that relate to potential criminal offences within the meaning of art. 10 GDPR, the EDPB recommends to resort to the local processing of the data where the data subject has full control over the processing in question (see discussion on local processing in section 2.4). Indeed – except for some exceptions (see the case study on accidentology studies presented below in section 3.3) – external processing of data revealing criminal offences or other infractions is forbidden. Thus, according to the sensitivity of the data, strong security measures such as those described in section 2.7 must be put in place in order to offer protection against the illegitimate access, modification and deletion of those data.
GDPR第10条の意味における潜在的な犯罪行為に関連するデータを取扱う場合に関し、EDPBは、データを車両内で取扱い、データ主体が問題となるデータの取扱いを完全に管理するよう勧告する（第2.4節の車両内での取扱いに関する説明を参照のこと）。実際、一部の例外（下記の第3.3節で示す事故調査事例のケース・スタディを参照のこと）を除き、犯罪行為又はその他の違反行為を示すデータを車両外部で取扱うことは許されない。したがって、当該データの機微性に鑑み、当該データへの違法アクセス、改変及び消去からデータを守るために、第2.7節で説明されているような強力な安全管理措置を講じなければならない。

68. Indeed, some categories of personal data from connected vehicles could reveal that a criminal offence or other infraction has been or is being committed ("offence-related data") and therefore be subject to special restrictions (e.g., data indicating that the vehicle crossed a white line, the instantaneous speed of a vehicle combined with precise location data). Notably, in the event that such data would be processed by the competent national authorities for the purposes of criminal investigation and prosecution of criminal offence, the safeguards provided for in art. 10 GDPR would apply.
実際、コネクテッドビークルから得られる一部の種類の個人データから、犯罪行為若しくはその他の違反行為が行われたか、又は行われていること（「犯罪関連データ」）が判明する可能性があり、したがって特別な制限の対象となる場合がある（例えば、車両が白線を越えたことを示すデータ、正確な位置データと組合わされた車両の瞬間速度を示すデータ）。特に、刑事捜査及び犯罪行為の訴追目的で当該データが国内所管官庁により取扱われる場合、GDPR第10条で規定される保護措置が適用される。

2.2 Purposes
目的

69. Personal data may be processed for a wide variety of purposes in relation to connected vehicles, including driver safety, insurance, efficient transportation, entertainment or information services. In accordance with the GDPR, data controllers must ensure that their purposes are "specified, explicit and legitimate", not further processed in a way incompatible with those purposes and that there is a valid legal basis for the processing as required in art. 5 GDPR. Some concrete examples of purposes that may be pursued by data controllers operating in the context of connected vehicles are discussed in Part III of these guidelines, along with specific recommendations for each type of processing.

コネクテッドビークルに関連して個人データは、運転者の安全、保険、効率的な輸送、娯楽、情報サービスなどの多様な目的で取扱われうる。データ管理者はGDPRに従い、取扱いの目的が「特定され、明確であり、かつ、正当な目的のため」であり、かつ、その目的と適合しない態様で追加的に取扱われないよう確保し、またGDPR第5条で要求されているように取扱いのための有効な法的根拠を備えるよう確保しなければならない。本ガイドラインの第3章では、コネクテッドビークルに関連する業務を行うデータ管理者が求めうるデータ取扱いの目的の具体例を、取扱いの類型ごとの勧告とともに検討する。

2.3 Relevance and data minimization
関連性及びデータの最小化

70. To comply with the data minimization principle[38], vehicle and equipment manufacturers, service providers and other data controllers should pay special attention to the categories of data they need from a connected vehicle, as they shall only collect personal data that are relevant and necessary for the processing. For instance, location data are particularly intrusive and can reveal many life habits of the data subjects. Accordingly, industry participants should be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing (see discussion on location data above, in section 2.1).
車両及び機器のメーカー、サービスプロバイダー、並びにその他のデータ管理者は、データ最小化の原則を遵守するため[38]、取扱いに関連しかつ必要な個人データに限り収集するよう、コネクテッドビークルから取得する必要のあるデータの種類に特段の注意を払うべきである。例えば、位置データは特に侵害的であり、データ主体の生活習慣の多くを明らかにしうる。したがって、業界の参加者は、取扱いの目的に照らして、位置データを収集することが絶対に必要な場合を除き、当該データを収集しないよう特に注意するべきである（上記第2.1節の位置データに関する説明を参照のこと）。

2.4 Data protection by design and by default
データ保護バイデザイン及びデータ保護バイデフォルト

71. Taking into account the volume and diversity of personal data produced by connected vehicles, the EDPB notes that data controllers are required to ensure that technologies deployed in the context of connected vehicles are configured to respect the privacy of individuals by applying the obligations of data protection by design and by default as required by art. 25 GDPR. Technologies should be designed to minimize the collection of personal data, provide privacy-protective default settings and ensure that data subjects are well informed and have the option to easily modify configurations associated with their personal data. Specific guidance on how manufacturers and service providers can comply with data protection by design and by default could be beneficial for the industry and third-party application providers.
コネクテッドビークルにより生成される個人データの量及び多様性を考慮し、EDPBは、データ管理者が、GDPR第25条で要求されているデータ保護バイデザイン及びデータ保護バイデフォルトの義務を適用することにより、コネクテッドビークルに関連して導入される技術を個人のプライバシーが尊重されるように構成しなければならない点に留意する。技術は、個人データの収集を最小限に抑え、初期設定としてプライバシー保護を提供し、かつデータ主体が十分な説明を受け、当該データ主体の個人データに関連付けられた設定を容易に変更するための選択肢が与えら

[38] GDPR, Article 5(1)(c).
GDPR第5条(1)(c)。

れることを確保するように設計するべきである。メーカー及びサービスプロバイダーがどのようにデータ保護バイデザイン及びデータ保護バイデフォルトに適合しうるかについて具体的な指針を示すことは、業界及び第三者のアプリケーション・プロバイダーにとって有益である可能性がある。

72. Certain general practices, described below, can also help mitigate the risks to the rights and freedoms of natural persons associated with connected vehicles[39].
また、以下で説明するいくつかの一般的な慣行も、コネクテッドビークルに関連する自然人の権利及び自由に対するリスクを軽減させうる[39]。

2.4.1 Local processing of personal data
個人データの車両内での取扱い

73. In general, vehicle and equipment manufacturers, service providers and other data controllers should, wherever possible, use processes that do not involve personal data or transferring personal data outside of the vehicle (i.e., the data is processed internally). The nature of connected vehicles however does present risks, such as the possibility of attacks on local processing by outside actors or local data being leaked by selling parts of the vehicle. Therefore, adequate attention and security measures should be taken into account to ensure that local processing shall remain local. This scenario offers the advantage of guaranteeing to the user the sole and full control of his/her personal data and, as such, it presents, "by design", less privacy risks especially by prohibiting any data processing by stakeholders without the data subject knowledge. It also enables the processing of sensitive data such as biometric data or data relating to criminal offenses or other infractions, as well as detailed location data which otherwise would be subject to stricter rules (see below). In the same vein, it presents fewer cybersecurity risks and involves little latency, which makes it particularly suited to automated driving-assistance functions. Some examples of this type of solution could include:
一般に、車両及び機器のメーカー、サービスプロバイダー、並びにその他のデータ管理者は、可能な限り、個人データを伴わない取扱い、又は車両外への個人データの移転を伴わない（つまり、データが車両内で取扱われるような）取扱方法を利用するべきである。しかしながら、コネクテッドビークルの性質上、車両内での取扱いが外部の行為主体から攻撃を受ける可能性、又は車両の部品を販売することにより車両内のデータが漏洩する可能性などのリスクが存在する。したがって、車両内での取扱いが車両内にとどまるよう確保するための適切な注意及び安全管理措置が考慮されるべきである。そうすることで、ユーザーに対して自己の個人データの唯一かつ完全な管理を保証するという利点がもたらされ、また特にデータ主体が知らない状態でのステークホルダーによるデータの取扱いを妨げることでプライバシーへのリスクを「バイデザインで」軽減することになる。加えて、生体データ、又は犯罪行為若しくはその他の違反行為に関連するデータなどのセンシティブなデータ、及び本来であればより厳格なルールが適用されるべき詳細な位置データを取扱うことも可能になる（以下を参照のこと）。同様にサイバーセキュリティのリスクが少なく、またレイテンシが小さいため、自動化された運転支援機能に特に適している。この種の方式の例には次のものがある。

- ☐ eco-driving applications that process data in the vehicle in order to display eco-driving advice in real time on the on-board screen;
- エコドライブに関する助言を車載画面にリアルタイムで表示するために、データを

[39] See as well European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020 (hereinafter - "Guidelines 4/2019").
また同様にEDPB、「第25条 データ保護バイデザイン及びデータ保護バイデフォルトに関するガイドライン04/2019」、バージョン 2.0、2020年10月20日採択（以下「ガイドライン04/2019」）も参照のこと。

車両内で取扱うエコドライブ・アプリケーション。

☐ applications that involve a transfer of personal data to a device such as a smartphone under the user's full control (via, for example, Bluetooth or Wi-Fi), and where the vehicle's data are not transmitted to the application providers or the vehicle manufacturers; this would include, for instance, coupling of smartphones to use the car's display, multimedia systems, microphone (or other sensors) for phone calls, etc., to the extent that the data collected remain under the control of the data subject and is exclusively used to provide the service he or she has requested;

・ （BluetoothやWi-Fiなどを介して）スマートフォンなどのユーザーが完全に管理するデバイスへ個人データを移転し、かつ車両のデータがアプリケーションのプロバイダー又は自動車メーカーに移転されないアプリケーション。例えば、スマートフォンを車載ディスプレイ、マルチメディアシステム、通話用のマイク（又はその他のセンサー）とつなげるものが該当し、収集されるデータがデータ主体の管理下にとどまり、データ主体が要求するサービスを提供するためにのみ利用されるもの。

☐ in-vehicle safety enhancing applications such as those that provide audible signals or vibrations of the steering wheel when a driver overtakes a car without indicating or straying over white lines or which provides alerts as to the state of the vehicle (e.g., an alert on the wear and tear affecting brake pads);

・ 安全性を高める車載アプリケーションで、例えば、運転者が信号を出さずに他の車を追い越そうとする際若しくは誤って白線を越える際に、音声信号を発するか若しくは車のハンドルを振動させるアプリケーション、又は（例えばブレーキパッドに影響を及ぼす摩耗警告など）車両の状態を警告するアプリケーション。

☐ applications for unlocking, starting, and/or activating certain vehicle commands using the driver's biometric data that is stored within the vehicle (such as a face or voice models or fingerprint minutiae).

・ 車両内に保存されている運転者の生体データ（顔又は音声識別モデル、指紋の特徴点など）を使い、車両のロックを解除する、エンジンを始動する、及び／又は一定の車両コマンドを起動するためのアプリケーション。

74. Applications such as the above involve processing carried out for the performance of purely personal activities by a natural person (i.e., without the transfer of personal data to a data controller or data processor). Therefore, in accordance with art. 2(2) GDPR, **these applications fall outside the scope of the GDPR.**
上記のようなアプリケーションの場合、自然人によって純粋に私的な行為を行うためにデータが取扱われる（つまり個人データがデータ管理者又はデータ処理者に移転されない）。したがって、**これらのアプリケーションは**GDPR第2条(2)に従い、**GDPRの適用範囲外である。**

75. However, if the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity, it does apply to controllers or processors, which provide the means for processing personal data for such personal or household activities (car manufacturers, service provider, etc.) in accordance with recital 18 GDPR. Hence, when they are acting as data controller or data processor, they must develop secure in-car application and with due respect to the principle of privacy by design and by default. In any case, according to recital 78 GDPR, *"When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data*

protection obligations".[40] One the one hand, it will enhance the development of user-centric services and, on the other hand, it will facilitate and secure any further uses in the future which could fall back within the scope of the GDPR. More specifically, the EDPB recommends developing a secure in-car application platform, physically divided from safety relevant car functions so that the access to car data does not depend on unnecessary external cloud capabilities.
しかしながら、自然人によって純粋に私的な行為又は家庭内の行為の過程において行われる個人データの取扱いであるため、その取扱いに対してGDPRが適用されない場合でも、GDPR前文第18項に従い、そのような私的な行為又は家庭内の行為のために個人データの取扱いの手段を提供する（自動車メーカー、サービスプロバイダーなどの）管理者又は処理者にはGDPRが適用される。したがって、メーカー及びサービスプロバイダーは、データ管理者又はデータ処理者として行為する際に、安全な車載アプリケーションを開発し、またプライバシー保護バイデザイン及びプライバシー保護バイデフォルトの原則を尊重しなければならない。いずれにせよ、GDPR前文第78項によれば、「*個人データの取扱いを基盤とし、又は、その職務を遂行するために個人データを取扱うアプリケーション、サービス及び製品を開発、設計、選択及び利用する場合、そのような製品、サービス及びアプリケーションの開発者は、そのような製品、サービス及びアプリケーションを開発及び設計する際、データ保護の権利を考慮に入れることが奨励され、また、最新技術を適正に考慮に入れた上で、管理者及び処理者がそのデータ保護義務を履行できるようにすることが奨励されなければならない*」[40]。そうすることで、一方でユーザー中心のサービスの開発を強化し、他方でGDPRの適用対象になる可能性のある将来的なデータの更なる使用を促進、確保することになろう。より具体的に言えば、EDPBは、車両データへのアクセスをする際に不要な外部クラウド機能に依存しないよう、安全関連の車両機能から物理的に分離された安全な車載アプリケーション・プラットフォームを開発するよう勧告する。

76. Local data processing should be considered by car manufacturers and service providers, whenever possible, to mitigate the potential risks of cloud processing, as they are underlined in the opinion on Cloud Computing released by the Article 29 Working Party.[41]
第29条作業部会が発表したクラウドコンピューティングに関する意見で強調されているように、自動車メーカー及びサービスプロバイダーは、クラウドによる取扱いに伴う潜在的なリスクを軽減するためにデータを極力車両内で取扱うよう検討するべきである[41]。

77. In general users should be able to control how their data are collected and processed in the vehicle:
一般的に、以下の手段により、自己のデータが車両内で収集され、取扱われる方法をユーザーが管理できるようにするべきである。

- information regarding the processing must be provided in the driver's language (manual, settings, etc.);
- 取扱いに関する情報（マニュアル、設定など）が運転者の使用言語で提供されること。

[40] For more recommendations on privacy by design and privacy by default see also Guidelines 4/2019.
プライバシーバイデザイン及びプライバシーバイデフォルトに関するその他の勧告に関しては「ガイドライン04/2019」も参照のこと。
[41] Article 29 Working Party – Opinion 5/2012 on Cloud Computing; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.
第29条作業部会、「クラウドコンピューティングに関する意見05/2012」、https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

- the EDPB recommends that only data strictly necessary for the functioning of the vehicle are processed by default. Data subjects should have the possibility to activate or deactivate the data processing for each other purpose and controller/processor and have the possibility to delete the data concerned, taking into account the purpose and the legal basis of the data processing ;
- EDPBは、初期設定で取扱われるデータを、車両機能に厳密に必要なデータのみに限定するよう勧告する。データ主体は、データ取扱いの目的及び管理者／処理者ごとに、データの取扱いを有効又は無効にすることができなければならない。またデータ主体は、データの取扱いの目的及び法的根拠を考慮し、当該データを消去できなければならない。

- data should not be transmitted to any third parties (i.e., the user has sole access to the data);
- データが第三者に移転されない（つまり、データにアクセスできる者をユーザーに限定する）こと。

- data should be retained only for as long as is necessary for the provision of the service or otherwise required by Union or Member State law;
- サービスの提供に必要な期間又はEU法若しくは加盟国の国内法で要求されている期間に限りデータが保存されること。

- data subjects should be able to delete permanently any personal data before the vehicles are put up for sale;
- 車両が売りに出される前にデータ主体が個人データを完全に消去できること。

- data subjects should, where feasible, have a direct access to the data generated by these applications.
- 可能な場合には、データ主体がこれらのアプリケーションにより生成されるデータに直接アクセスできるようにすること。

78. Finally, while it may not always be possible to resort to local data processing for every use-case, “hybrid processing” can often be put in place. For instance, in the context of usage-based insurance, personal data regarding driving behaviour (such as the force exerted on the brake pedal, mileage driven, etc.) could either be processed inside the vehicle or by the telematics service provider on behalf of the insurance company (the data controller) to generate numerical scores that are transferred to the insurance company on a defined basis (e.g. on a monthly basis). In this way, the insurance company does not gain access to the raw behavioral data but only to the aggregate score that is the result of the processing. This ensures that principles of data minimization are satisfied by design. This also means that users must have the ability to exercise their right when data are stored by other parties: for example, a user should have the ability to delete data stored in the systems of a car maintenance shop or dealership under the conditions of art.17 GDPR.
最後に、あらゆる使用例についてデータの車両内での取扱いが常に可能であるとは限らないものの、「ハイブリッドな取扱い」を導入できる場合も多い。例えば、利用ベース型保険の場合、（月1回など）所定の時間間隔で保険会社に移転される数値スコアを生成するために（ブレーキペダルにかかる力、走行距離などの）運転行動に関する個人データを車両内で取扱う方法、又は保険会社（データ管理者）の代わりにテレマティクス・サービスのプロバイダーが取扱う方法もある。このような方法であれば、保険会社が生の行動データにアクセスせず、取扱いの結果としての集約されたスコアへのアクセスに限定できる。これにより、データ最小化の原則がバイデザインで満たされるよう確保できる。このことはまた、データが別の者により保存されている場合に、自己の権利を行使する能力をユーザーが有しなければならないことを意味する。つまり、例えば、自動車整備工場又は販売店のシステムに自己のデータが保存されている場合、GDPR第17条の条件に基づきデータを消去す

る能力をユーザーが有していなければならない。

2.4.2 Anonymization and pseudonymization
匿名化及び仮名化

79. If the transmission of personal data outside the vehicle is envisaged, consideration should be given to anonymize them before being transmitted. When anonymizing the controller should take into account all processing involved which could potentially lead to re-identification of data, such as the transmission of locally anonymized data. The EDPB recalls that the principles of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable[42]. Once a dataset is truly anonymized and individuals are no longer identifiable, European data protection law no longer applies. As a consequence, anonymization, where relevant, may be a good strategy to keep the benefits and to mitigate the risks in relation to connected vehicles.
個人データの車両外への移転が想定される場合、移転前にデータを匿名化することを検討するべきである。管理者は、匿名化する際には、車両内で匿名化されたデータの移転など、データの再識別につながる可能性のある、関連するあらゆる取扱いを考慮するべきである。EDPBは、データ保護の基本原則が、匿名情報、すなわち、識別された自然人又は識別可能な自然人との関係をもたない情報、又は、データ主体を識別できないように匿名化された個人データに対しては、適用されない点を想起する[42]。データセットが真に匿名化され、個人を識別できなくなると、欧州データ保護法令は適用されなくなる。結果として、匿名化は、適切なときは、コネクテッドビークルの利点を維持しつつリスクを軽減するための優れた戦略となりうる。

80. As detailed in the opinion by the Article 29 Working Party on anonymization techniques, various methods can be used – sometimes in combination – in order to reach data anonymisation[43].
匿名化技法に関する第29条作業部会の意見に詳述されているように、データの匿名化をするために多様な方法を（時には組み合わせて）利用することができる[43]。

81. Other techniques such as pseudonymization[44] can help minimize the risks generated by the data processing, taking into account that in most cases, directly identifiable data are not necessary to achieve the purpose of the processing. Pseudonymization, if reinforced by security safeguards, improves the protection of personal data by reducing the risks of misuse. Pseudonymization is reversible, unlike anonymization, and pseudonymized data are considered as personal data subject to the GDPR.
取扱いの目的を達成するために直接的に識別可能なデータが必要とされない場合が大半であることを考慮すれば、仮名化[44]などの他の技法もデータの取扱いから生ずるリスクを最小限に抑える助けになりうる。仮名化は、安全管理上の保護措置により補強されれば、不正使用のリスクが軽減され、個人データの保護を向上させる。仮名化は匿名化とは異なり可逆的であり、仮名化されたデータはGDPRが適用され

[42] See GDPR, Article 4 (1) and Recital 26.
GDPRの第4条(1)及び前文第26項を参照のこと。
[43] WP29 - Opinion 05/2014 on Anonymization Techniques; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
第29条作業部会、「匿名化技法に関する意見05/2014」、https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[44] GDPR, Article 4 (5). Enisa report on December 03, 2019: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.
GDPR第4条(5)。2019年12月3日のEnisa報告書、https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

る個人データとみなされる。

2.4.3 Data protection impact assessments
データ保護影響評価

82. Given the scale and sensitivity of the personal data that can be generated via connected vehicles; it is likely that processing - particularly in situations where personal data are processed outside of the vehicle - will often result in a high risk to the rights and freedoms of individuals. Where this is the case, industry participants will be required to perform a data protection impact assessment (DPIA) to identify and mitigate the risks as detailed in art. 35 and 36 GDPR. Even in the cases where a DPIA is not required, it is a best practice to conduct one as early as possible in the design process. This will allow industry participants to factor the results of this analysis into their design choices prior to the roll-out of new technologies.
コネクテッドビークルを介して生成されうる個人データの規模及び機微性を考慮すると、特に個人データが車両外で取扱われる状況において、取扱いが個人の権利及び自由への高いリスクを発生させるおそれがある場合が多い。その場合、業界の参加者は、GDPR第35条及び第36条で詳しく規定しているように、リスクを特定し、軽減するためにデータ保護影響評価（DPIA）を実行する必要がある。DPIAが必要とされない場合でも、設計過程の極力早い段階でDPIAを実行することが最も望ましい慣行である。業界の参加者は、そうすることで、新技術を展開する前の設計の選択の段階で当該分析結果を織り込むことができる。

2.5 Information
情報

83. Prior to the processing of personal data, the data subject shall be informed of the identity of the data controller (e.g., the vehicle and equipment manufacturer or service provider), the purpose of processing, the data recipients, the period for which data will be stored, and the data subject's rights under the GDPR[45].
データ主体は、個人データが取扱われる前に、データ管理者（例えば車両及び機器のメーカー又はサービスプロバイダー）の身元、取扱いの目的、データの取得者、データが保存される期間、及びGDPRに基づくデータ主体の権利に関する説明を受ける[45]。

84. In addition, the vehicle and equipment manufacturer, service provider or other data controller should also provide the data subject with the following information, in clear, simple, and easily-accessible terms:
加えて、車両及び機器のメーカー、サービスプロバイダー、又はその他のデータ管理者は、データ主体に対し、以下の情報を明確で、平易で、かつ容易にアクセスできる方式で提供するべきである。

☐ the contact details of the data protection officer;
- データ保護オフィサーの連絡先。

☐ the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- 予定されている個人データの取扱いの目的及びその取扱いの法的根拠。

☐ the explicit mention of the legitimate interests pursued by the data controller or by a third

[45] GDPR, Article 5 (1) (a) and 13. See also Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), endorsed by the EDPB.
GDPR第5条(1)(a)及び第13条。また、第29条作業部会、「規則2016/679に基づく透明性に関するガイドライン」、 WP260rev.01、EDPB承認版も参照のこと。

party, when such legitimate interests constitute the legal basis for processing;
- 正当な利益をデータの取扱いの法的根拠とする場合、当該データ管理者又は第三者が求める正当な利益への明確な言及。

☐ the recipients or categories of recipients of the personal data, if any;
- もしあれば、個人データの取得者又は取得者の類型。

☐ the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- その個人データが記録保存される期間、又は、それが不可能なときは、その期間を決定するために用いられる基準。

☐ the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- 個人データへのアクセス、個人データの訂正又は消去、又は、データ主体と関係する取扱いの制限を管理者から得ることを要求する権利、又は、取扱いに対して異議を述べる権利、並びに、データポータビリティの権利が存在すること。

☐ the existence of the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal where the processing is based on consent;
- データの取扱いが同意に基づく場合、その撤回前の同意に基づく取扱いの適法性に影響を与えることなく、いつでも同意を撤回する権利が存在すること。

☐ where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and safeguards used to transfer them;
- 該当する場合は、管理者が個人データを第三国又は国際機関に移転することを予定しているという事実、及び、データを移転するために利用する保護措置。

☐ whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- その個人データの提供が制定法上若しくは契約上の要件であるか否か、又は、契約を締結する際に必要な要件であるか否か、並びに、データ主体がその個人データの提供の義務を負うか否か、及び、そのデータの提供をしない場合に生じうる結果について。

☐ the existence of automated decision-making, including profiling that produces legal effects concerning the data subject or similarly significantly affects the data subject, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. This could particularly be the case in relation to the provision of usage-based insurance to individuals;
- データ主体に関する法的効果を発生させる、又は、データ主体に対して同様の重大な影響を及ぼすプロファイリングを含め、自動的な決定が存在すること、また、その決定に含まれている論理、並びに、当該取扱いのデータ主体への重要性及びデータ主体に生ずると想定される結果に関する意味のある情報。これは、特に個人を対象として利用ベース型保険を提供する場合に当てはまりうる。

☐ the right to lodge a complaint with a supervisory authority;
- 監督機関に異議を申立てる権利。

☐ information about further processing;
- 追加的取扱いに関する情報。

☐ In case of joint data controllership, clear and complete information about the responsibilities of each data controller.

・共同データ管理者の場合には、各データ管理者の責任に関する明確かつ完全な情報。

85. In some cases, personal data is not collected directly from the individual concerned. For instance, a vehicle and equipment manufacturer may rely on a dealer to collect information about the owner of the vehicle in order to offer an emergency road side assistance service. When data have not been collected directly, the vehicle and equipment manufacturer, service provider or other data controller shall, in addition to the information mentioned above, also indicate the categories of personal data concerned, the source from which the personal data originate, and, if applicable, whether those data came from publicly accessible sources. That information must be provided by the controller within a reasonable period after obtaining the data, and **no later than the first of the following dates** in accordance with art. 14 (3) GDPR: (i) one month after the data are obtained, having regard to the specific circumstances in which the personal data are processed, (ii) upon first communication with the data subject, or (iii) if those data are transmitted to a third party, before the transmission of the data.
個人データが、関係する個人から直接収集されないケースもある。例えば、車両及び機器のメーカーは、緊急時のロードアシスタンスサービスを提供する目的で車両の所有者に関する情報を収集するために販売店に頼る場合がある。データが直接収集されていない場合、車両及び機器のメーカー、サービスプロバイダー、又はその他のデータ管理者は、上記の情報に加え、当該個人データの種類、その個人データを得た情報源、及び、該当する場合は、公衆がアクセス可能な情報源からその個人データが来たものかどうかの情報を提示する。当該情報は、GDPR第14条(3)に従い、データ取得後の合理的な期間内に、ただし、**次の日付のいずれか早い日までに**管理者により提供されなければならない。（i）その個人データが取扱われる具体的な状況を考慮に入れ、データ取得後1か月以内、(ii)当該データ主体に対して最初の連絡がなされる時点、又は(iii)当該個人データが第三者に移転される場合にはデータの移転前。

86. New information may also need to be provided to data subjects when they are taken care of by new data controller. A roadside assistance service that interacts with connected vehicles can be provided by different data controllers depending in which country or region the assistance is required. New data controllers should provide data subjects with the required information when data subjects cross borders and services that interact with connected vehicles are provided by new data controllers.
また、新規のデータ管理者がデータ主体を担当する場合には、その際に新規情報をデータ主体に提供する必要が生じうる。ロードアシスタンスサービスが必要となる国や地域に応じ、コネクテッドビークルと連携するロードアシスタンスサービスが、多様なデータ管理者により提供されうる。データ主体が国境を越える場合、新規のデータ管理者が必要な情報をデータ主体に提供すべきであり、コネクテッドビークルと連携するサービスは新たなデータ管理者により提供される。

87. The information directed to the data subjects may be provided in layers[46], i.e. by separating two levels of information: on the one hand, first-level information, which is the most important for the data subjects, and, on the other hand, information that presumably is of interest at a later stage. The essential first-level information includes, in addition to the identity of the data controller, the purpose of the processing and a description of the data subject’s rights, as well as any additional information on the processing which has the most impact on the data subject and processing which could surprise them. The EDPB recommends that, in the context of connected vehicles, the data subject should be made aware of all the recipients in the first layer of information. As stated in the WP29 guidelines

on transparency, controllers should provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers cannot provide the names of the recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector, and the location of the recipients.
データ主体に提示される情報は、階層的に[46]、つまり次のような二階層の情報に分けて提供しうる。具体的には、まず第一階層の情報として、データ主体にとって最も重要な情報を、次に、恐らくは後の段階で関心を持たれる情報を提供する。第一階層の必須情報は、データ管理者の身元に加え、取扱いの目的及びデータ主体の権利の説明、並びにデータ主体への影響が最も大きな取扱い及びデータ主体にとって不意打ちとなりかねない取扱いといったあらゆる追加情報を含む。EDPBは、コネクテッドビークルに関し、データ主体が情報の第一階層で、全てのデータ取得者に関する情報を知らされるべきであると勧告している。第29条作業部会の透明性に関するガイドラインに記載されているように、管理者は、データ主体にとって最も意味のある、取得者に関する情報を提供するべきである。実際には、データ主体が自己の個人データを保有する者を正確に知ることができるよう、一般に、取得者の氏名がこれに該当する。管理者が取得者の氏名を提示できない場合には、（取得者が実施する活動に言及することによる）取得者の種類、業界、産業部門及び産業部門の下位区分、及び取得者の所在地を示すなど、できる限り具体的な情報を提示すべきである。

88. The data subjects may be informed by concise and easily understandable clauses in the contract of sale of the vehicle, in the contract for the provision of services, and/or in any written medium, by using distinct documents (e.g., the vehicle's maintenance record book or manual) or the on-board computer.
データ主体は、簡潔でわかりやすい条項により車両の売買契約書、サービスの提供の契約書の中で及び／若しくは（例えば、車両の保守記録簿若しくはマニュアルなど）別文書を使用しなんらかの書面媒体の中で通知されるか、又は車載コンピューターを利用することにより通知されうる。

89. Standardized icons could be used in addition to the information necessary, as required under art. 13 and 14 GDPR, to enhance transparency by potentially reducing the need for vast amounts of written information to be presented to a data subject. It should be visible in vehicles in order to provide, in relation to the planned processing, a good overview that is understandable, and clearly legible. The EDPB emphasizes the importance of standardizing those icons, so that the user finds the same symbols regardless of the make or model of the vehicle. For example, when certain types of data are being collected, such as location, the vehicles could have a clear signal on-board (such as a light inside the vehicle) to inform passengers about data collection.
データ主体に対し、GDPR第13条及び第14条の要件である必要な情報提供に加え、透明性を高めるために、膨大な量の書面による情報を提示する必要性を潜在的に減らし、標準化したアイコンを使用することが考えられるであろう。予定されているデータの取扱いに関し、理解可能で明確に判読可能な概要を提供するために、車両内で視認できるものとすべきである。EDPBは、ユーザーが車両の型式や年式に関係なく同じ記号を目にするよう、当該アイコンを標準化することの重要性を強調す

[46] See Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), endorsed by the EDPB.
第29条作業部会、「規則2016/679に基づく透明性に関するガイドライン」、 WP260 rev.01、EDPB承認版を参照のこと。

る。例えば、位置などの一定の種類のデータが収集される場合には、データの収集が行われていることを同乗者に通知するために、（車両内のライトを点灯するなど）明確に合図するものを車両に搭載することが考えられる。

2.6 Rights of the data subject
データ主体の権利

90. Vehicle and equipment manufacturers, service providers and other data controllers should facilitate data subjects' control over their data during the entire processing period, through the implementation of specific tools providing an effective way to exercise their rights, in particular their right of access, rectification, erasure, their right to restrict the processing and, depending on the legal basis of the processing, their right to data portability and their right to object.
車両及び機器のメーカー、サービスプロバイダー、並びにその他のデータ管理者は、データ主体の権利、特にアクセス、訂正、消去、取扱いの制限の権利、並びに取扱いの法的根拠に応じてデータポータビリティの権利及び異議を述べる権利を、データ主体が効果的に権利行使できるような手段を備える具体的なツールを導入することにより取扱いの期間の全体を通してデータ主体による自己のデータの管理の促進を図るべきである。

91. To facilitate settings modifications, a profile management system should be implemented in order to store the preferences of known drivers and help them to change easily their privacy settings anytime. The profile management system should centralize every data setting for each data processing, especially to facilitate the access, deletion, removal and portability of personal data from vehicle systems at the request of the data subject. Drivers should be enabled to stop the collection of certain types of data, temporarily or permanently, at any moment, unless there is a specific legal ground that the controller can rely on to continue the collection of specific data. In case of a contract that provides a personalized offer based on driving behaviour this may mean that the user as a result should be reverted to the standard conditions of that contract. These features should be implemented inside the vehicle, although it could also be provided to data subjects through additional means (e.g., dedicated application). Furthermore, in order to allow data subjects to quickly and easily remove personal data that can be stored on the car's dashboard (for example, GPS navigation history, web browsing, etc.), the EDPB recommends that manufacturers provide a simple functionality (such as a delete button).
設定の変更を容易にするため、プロファイル管理システムを実装し、特定の運転者の好みを保存しつつ、かつ、当該運転者がいつでも容易に自己のプライバシー設定を変更できるようにするべきである。当該プロファイル管理システムは、特に、データ主体の要求に応じて、個人データのアクセス、車両システムからの消去（deletion）、削除（removal）、及びポータビリティが容易にできるようにし、取扱いデータ毎のデータ設定を一カ所にまとめるべきである。管理者がデータの収集の継続を正当化しうるような特定の法的根拠がない場合、運転者が随時、一定の種類のデータの収集を一時的又は恒久的に停止できるようにするべきである。もし運転行動連動型のパーソナライズされたサービスを提供する契約である場合、結果的にユーザーが標準的な契約条件に戻さなければならなくなる可能性がある。これらの機能は車両内で実施されるべきであるものの、（専用アプリケーションなどの）追加的手段を介してデータ主体に提供することも可能であると考えられる。さらに、EDPBは、データ主体が車のダッシュボードに保存されている可能性がある個人データ（GPSナビゲーション履歴、ウェブブラウジング履歴など）を迅速かつ容易に削除できるように、メーカーが（消去ボタンなどの）簡便な機能を配備するよう勧告する。

92. The sale of a connected vehicle and the ensuing change of ownership should also trigger the deletion of any personal data, which is no longer needed for the previous specified purposes and the data subject should be able to exercise his or her right to portability.
また、コネクテッドビークルの販売及びその後の所有権の変更時においても、以前の特定の目的のための、不要となった個人データを消去しなければならない。加えて、データ主体は当然、ポータビリティの権利の行使が可能であるべきである。

2.7 Security
安全管理

93. Vehicle and equipment manufacturers, service providers and other data controllers should put in place measures that guarantee the security and confidentiality of processed data and take all useful precautions to prevent control being taken by an unauthorized person. In particular, industry participants should consider adopting the following measures:
車両及び機器のメーカー、サービスプロバイダー、並びにその他のデータ管理者は、取扱われるデータの安全性及び機密性を保証する対策を講じるべきであり、権限のない人物による管理が行われないように、あらゆる有用な予防措置を講じるべきである。特に、業界の参加者は、次の対策を講じるよう検討すべきである。

☐ encrypting the communication channels by means of a state-of-the-art algorithm;
- 最先端のアルゴリズムを利用して通信チャネルを暗号化すること。

☐ putting in place an encryption-key management system that is unique to each vehicle, not to each model;
- 車種毎ではなく、各車両毎に固有の暗号鍵管理システムを導入すること。

☐ when stored remotely, encrypting data by means of state-of-the-art algorithms;
- 車外に保存する場合、最先端のアルゴリズムを使ってデータを暗号化すること。

☐ regularly renewing encryption keys;
- 暗号鍵を定期的に更新すること。

☐ protecting encryptions keys from any disclosure;
- 暗号鍵をいかなる開示からも保護すること。

☐ authenticating data-receiving devices;
- データ受信装置の認証システムを導入すること。

☐ ensuring data integrity (e.g., by hashing);
- （ハッシュ化などにより）データの完全性を確保すること。

☐ make access to personal data subject to reliable user authentication techniques (password, electronic certificate, etc.);
- 個人データへのアクセスに、信頼性のある技法（パスワード、電子証明など）によるユーザー認証を設けること。

94. Concerning more specifically vehicle manufacturers, the EDPB recommends the implementation of the following security measures:
特に自動車メーカーに関して、EDPBは、以下の安全管理措置を導入するよう勧告する。

☐ partitioning the vehicle's vital functions from those always relying on telecommunication capacities (e.g., "infotainment");
- 車両の運転上重要な機能を、情報通信機能に常時依存している（「インフォテインメント」などの）機能から分離すること。

☐ implementing technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle;
- 自動車メーカーが車両の耐用期間全体にわたって安全管理上の脆弱性に迅速にパッチを当てることを可能にするような技術上の対策を導入すること。

☐ for the vehicle's vital functions, give priority as much as possible to using secure means of communications that are specifically dedicated to transportation;
- 車両の運転上重要な機能に関しては、特別に輸送用に設けられた安全な通信手段を利用することを極力優先させること。

☐ setting up an alarm system in case of attack on the vehicle's systems, with the possibility of operating in downgraded mode[47];
- 車両のシステムが攻撃された場合にそのことを知らせる警報システムを装備すること。その際に車両のシステムをダウングレードしたモードで動作させることが可能なものとすること[47]。

☐ storing a log history of any access to the vehicle's information system, e.g. going back six months as a maximum period, in order to enable the origin of any potential attack to be understood and periodically carry out a review of the logged information to detect possible anomalies.
- 潜在的な攻撃の原因に関して理解し、また障害の可能性を検出する目的で記録された情報を定期的に確認するために、例えば最長で6か月前まで遡り、車両の情報システムへのアクセスのログ履歴を保存すること。

95. These general recommendations should be completed by specific requirements taking into account the characteristics and purpose of each data processing.
上記一般勧告を、データ取扱い毎の特性及び目的を考慮した特定の要件により補完すべきである。

2.8 Transmitting personal data to third parties
個人データの第三者への移転

96. In principle, only the data controller and the data subject have access to the data generated by a connected vehicle. However, the data controller may transmit personal data to a commercial partner (recipient), to the extent that such transmission lawfully relies on one of the legal bases stated in art. 6 GDPR.
コネクテッドビークルにより生成されるデータにアクセスできるのは原則としてデータ管理者とデータ主体のみである。しかしながら、データ管理者は、個人データの移転がGDPR第6条に規定される法的根拠のいずれかに基づき適法な場合に限り、当該データを商業的なパートナー（取得者）に移転しうる。

97. In view of the possible sensitivity of the vehicle-usage data (e.g., journeys made, driving style), the EDPB recommends that the data subject's consent be systematically obtained before their data are transmitted to a commercial partner acting as a data controller (e.g., by ticking a box that is not pre-ticked, or, where technically possible, by using a physical or logical device that the person can access from the vehicle). The commercial partner in turn

[47] Downgraded mode is a vehicle operating mode ensuring that the functions essential for the safe operation of the vehicle (i.e., minimum safety requirements) would be guaranteed, even if other less important functionalities would be deactivated (e.g., the operation of the geo-guidance device can be considered as non- essential, as opposed to the braking system).
ダウングレードされたモードとは、他の重要性の低い機能（例えばブレーキシステムとは異なり、ジオガイダンス装置の運用は必須ではないとみなしうる）が解除された場合でも車両の安全な運行に不可欠な機能（つまり最小限の安全要件）が保証されるよう確保できるような車両運行モードである。

becomes responsible for the data that it receives, and is subject to all the provisions of the GDPR.
EDPBは、車両使用データ（例えば走行ルート、運転スタイル）の機微性を考慮し、データ管理者として行為する商業的なパートナーにデータを移転する前に、（例えば事前にチェックが入っていないチェックボックスにチェックマークを付けるか、技術的に可能であれば、データ主体が車両からアクセスできる物理的又は論理的なデバイスを利用することにより）データ主体の同意を取得するための仕組みをシステムに組み込んでおくよう勧告する。代わって今度は当該商業的なパートナーが、取得したデータに責任を負い、GDPRのあらゆる規定を遵守することになる。

98. The vehicle manufacturer, service provider or other data controller can transmit personal data to a data processor selected to play a part in providing the service to the data subject, provided the data processor shall not use those data for its own purpose. Data controllers and data processors shall draw up a contract or other legal document specifying the obligations of each party and setting out the provisions of art. 28 GDPR.
自動車メーカー、サービスプロバイダー、又はその他のデータ管理者は、データ主体へのサービスの提供に参加する者として選定されたデータ処理者に個人データを移転できる。ただし、当該データ処理者は、当該データを独自の目的で使用しないものとする。データ管理者及びデータ処理者は、各当事者の義務を明記し、GDPR第28条の条項を入れた契約書又はその他の法的文書を作成する。

2.9 Transfer of personal data outside the EU/EEA
個人データのEU／EEA域外への移転

99. When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data.
個人データが欧州経済領域外に移転される場合、データの保護が維持されるよう確保するために特別な保護措置を講ずる必要性が予想される。

100. As a consequence, the data controller may transfer personal data to a recipient only to the extent that such transfer is in accordance with the requirements laid down in Chapter V GDPR.
結論としては、データ管理者は、個人データの移転がGDPR第5章に定められた要件に従って行われる場合にのみ当該データを取得者に移転できることになる。

2.10 Use of in-vehicle Wi-Fi technologies
車載Wi-Fi技術の使用

101. Advances in cellular technology have made it possible to easily use the Internet on the road. While it is possible to get Wi-Fi connectivity in a vehicle through a smartphone hotspot or a dedicated device (OBD-II dongle, wireless modem or router, etc.), most manufacturers offer nowadays models that include a built-in cellular data connection and are also capable of creating Wi-Fi networks. Depending on the case, various aspects must be considered:
セルラー技術の進歩により、走行中にインターネットを容易に利用することが可能になった。スマートフォンのホットスポット機能又は車両専用装置（OBD2ドングル、無線モデム又はルーターなど）を介して車両内でWi-Fi接続を確立することは可能であるものの、大半のメーカーは現在、モバイルデータ接続機能を搭載し、かつ、Wi-Fiネットワークを構築できる車種を販売している。それぞれのケースに応じて多様な側面を考慮しなければならない。

- ☐ The Wi-Fi connectivity is offered as a service by a road professional, such as a taxi driver for its customers. In this case, the professional or his/her company might be considered as an internet service provider (ISP), hence be subject to specific obligations and restrictions regarding the processing of his / her clients' personal data.

- タクシーの運転手が顧客向けに提供する場合など、Wi-Fi接続が道路輸送を専門とする者によりサービスとして提供されている場合。この場合、当該輸送を専門とする者又はその雇用会社は、インターネットサービスプロバイダー（ISP）とみなすことができ、それゆえに顧客の個人データの取扱いに関して特定の義務を負い、又特定の制限を受ける。

☐ The Wi-Fi connectivity is put in place for the sole use of the driver (at the exclusion of the driver and his/her passengers). In this case, the processing of personal data is considered to be purely personal or household activity in accordance with art. 2(2)(c) and recital 18 GDPR.
- 運転者のみが利用するために（運転者とその同乗者の両者が利用する場合は除く）Wi-Fi接続機能が搭載されている場合。この場合、個人データの取扱いは、GDPR第2条(2)(c)及びGDPR前文第18項に従った純粋に私的な行為又は家庭内の行為であるとみなされる。

102. In general, the proliferation of Internet connection interfaces via Wi-Fi poses greater risks to the privacy of individuals. Indeed, through their vehicles, users become continuous broadcasters, and can therefore be identified and tracked. In order to prevent tracking, easy to operate opt-out options ensuring the service set identifier (SSID) of the on-board Wi-Fi network is not collected should therefore be put in place by the vehicle and equipment manufacturers.
一般に、Wi-Fiを介したインターネット接続インターフェースの急速な普及は、個人のプライバシーに対するリスクの増大を招いている。ユーザーは、実際には自身の車両を通じて継続的な発信の担い手になり、したがって、識別され、追跡されうる。それゆえ、追跡されるのを防ぐために、車載Wi-Fiネットワークのサービスセット識別子（SSID）が収集されないよう確保すべく、操作が容易な機能停止オプションを車両及び機器のメーカーは搭載すべきである。

3 CASE STUDIES
ケース・スタディ

103. This section addresses five specific examples of processing in the context of connected vehicles, which correspond to scenarios likely to be encountered by stakeholders in the sector. The examples cover data processing that requires calculating power which cannot be mobilized locally in the vehicle, and/or the sending of personal data to a third party to carry out further analysis or to provide further functionality remotely. For each type of processing, this document specifies the intended purposes, the categories of data collected, the retention period of such data, the rights of data subjects, the security measures to be implemented, and the recipients of the information. In the case some of these fields are not described in the following, the general recommendations described in the previous part apply.
本節では、コネクテッドビークルに関連するデータ取扱いの五つの具体例を取扱う。これらは、当該業界のステークホルダーが遭遇する可能性の高いシナリオに対応したものである。これらの事例には、車両内で運用できないレベルの計算能力が必要とされるデータの取扱い及び／又は個人データを第三者に送信し、さらなる分析を行うか又はさらなる機能を遠隔的に提供するケースも含まれる。本ガイドラインでは、それぞれの取扱いの類型ごとに、想定されている目的、収集されるデータの種類、当該データの保存期間、データ主体の権利、導入されるべき安全管理措置、及び情報の取得者を明記する。これらの項目の一部が以下で説明されていない場合には、前章で説明した一般勧告があてはまる。

104. The examples chosen are non-exhaustive and are meant to be indicative of the variety of types of processing, legal bases, actors, etc. that might be engaged in the context of connected vehicles.
選定された事例は網羅的なものではなく、コネクテッドビークルに関与しうる多様な取扱いの類型、法的根拠、行為主体などの典型例を示すことを目的としている。

3.1 Provision of a service by a third party
第三者によるサービスの提供

105. Data subjects may contract with a service provider in order to obtain added-value services relating to their vehicle. For example, a data subject may enter into a usage-based insurance contract that offers reduced insurance premiums for less driving ("Pay As You Drive") or good driving behaviour ("Pay How You Drive") and which necessitates monitoring of driving habits by the insurance company. A data subject could also contract with a company that offers roadside assistance in the event of a breakdown and which entails the transmission of the vehicle's location to the company or with a service provider in order to receive messages or alerts relating to the vehicle's functioning (e.g., an alert on the state of brake wear, or a reminder of the technical-inspection date).
データ主体が、自己の車両に関連する付加価値サービスを受けるためにサービスプロバイダーと契約する場合がある。例えば、データ主体は利用ベース型保険契約を締結しうる。当該契約では、走行機会が少ない車両（「走行距離連動型保険」）又は良好な運転行動（「運転行動連動型保険」）に対し、減額保険料が提示されると同時に、保険会社による運転習慣の監視が必要となる。また、データ主体が、車の故障時に備えたロードアシスタンスサービスを提供する企業と、車両の位置を当該企業に移転する旨を含む契約を結ぶ場合、又は（例えばブレーキの摩耗状態に関する警告、若しくは定期点検日のリマインダーなど）車両の機能に関連するメッセージ若しくは警告を受信するためにサービスプロバイダーと契約する場合もある。

3.1.1 Usage-based insurance
利用ベース型保険

106. "Pay as you drive" is a type of usage-based insurance that tracks the driver's mileage and/or driving habits to differentiate and reward "safe" drivers by giving them lower premiums. The insurer will require the driver to install a built-in telematics service, a mobile application or activate a built-in module from manufacturing that tracks the miles covered and/or the driving behaviour (braking pattern, rapid acceleration, etc.) of the policy holder. The information gathered by the telematic device will be used to assign the driver scores in order to analyze what risks he/she may pose to the insurance company.
「走行距離連動型保険」は、運転者の走行距離及び／又は運転習慣を追跡し、「安全な」運転者を識別し、その保険料を減額する特典を与える利用ベース型保険の一種である。保険会社は、走行距離及び／又は保険契約者の運転行動（ブレーキのかけ方、急加速など）を追跡するために車載型テレマティクス・サービスを設置するか、モバイルアプリケーションをインストールするか、又は製造時に装備された車載型モジュールを起動することを運転者に要求する。テレマティック装置により収集される情報は、運転者が保険会社にどのようなリスクを生じさせうるかを分析する目的で運転者に運転スコアを割り当てるために利用される。

107. As usage-based insurance requires consent under art. 5(3) of the ePrivacy directive, the EDPB outlines that the policy holder must have the choice to subscribe to a non-usage-based insurance policy. Otherwise, consent would not be considered freely given, as the performance of the contract would be conditional on the consent. Further, art. 7(3) GDPR requires that a data subject must have the right to withdraw consent.
利用ベース型保険にはeプライバシー指令第5条(3)に基づく同意が必要とされるた

め、EDPBは、利用ベース型ではない保険契約に加入する選択肢が保険契約者に与えられなければならない旨、述べておく。そうでなければ、契約の履行が同意を条件とすることとなり、同意が自由に与えられたとはみなされない。加えて、GDPR第7条(3)に従い、データ主体は同意を撤回する権利を有しなければならない。

3.1.1.1 Legal basis
法的根拠

108. When the data is collected through a publicly available electronic communication service (for example *via* the SIM card contained in the telematics device), consent will be needed in order to gain access to information that is already stored in the vehicle as provided by art. 5(3) ePrivacy directive. Indeed, none of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user. Consent could be collected at the time of the conclusion of the contract.
公衆に利用可能な電子通信サービスを介して（例えばテレマティクス装置に含まれるSIMカードを介して）データが収集される場合、eプライバシー指令第5条(3)に規定されるように車両に既に保存されている情報へのアクセスを取得するには同意を得る必要がある。こうしたケースでは、同条項に定める適用除外のいずれも適用されない。つまり、当該取扱いは、電子通信ネットワークを介した通信の送信を実行することのみを目的とするものではなく、また、加入者又はユーザーから明確に要求された情報社会サービスに関連するものでもない。同意は、契約の締結時に得ることが可能である。

109. As regards the processing of personal data following the storage or access to the end-user's terminal equipment, the insurance company can rely on art. 6(1)(b) GDPR in this specific context provided it can establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed. Insofar as the processing is objectively necessary for the performance of the contract with the data subject, the EDPB considers that reliance upon art. 6(1)(b) GDPR would not have the effect of lowering the additional protection provided by art. 5(3) of the ePrivacy directive in this specific instance. That legal basis is materialized by the data subject signing a contract with the insurance company.
当該事例において、保険会社は、エンドユーザーの端末機器への保存又は当該機器へのアクセスに続く個人データの取扱いに関して、GDPR第6条(1)(b)を根拠とすることができる。ただし、データ主体との有効な契約に関連して当該取扱いが行われること、かつデータ主体との当該契約を履行するために当該取扱いが必要であることの両方を保険会社が立証できることが条件となる。EDPBは、データ主体との契約を履行するために当該取扱いが客観的に必要である限り、GDPR第6条(1)(b)を根拠としても、当該特定の事例においてeプライバシー指令第5条(3)により規定される追加的保護を引き下げる結果にはならないと考える。当該法的根拠は、データ主体が保険会社との契約に署名することにより成立する。

3.1.1.2 Data collected
収集されるデータ

110. There is two types of personal data to be considered:
考慮すべき個人データは次の2種類存在する。

- **commercial and transactional data**: data subject's identifying information, transaction-related data, data relating to means of payment, etc.;

- **商取引上のデータ：** データ主体の身元情報、取引関連データ、決済手段に関連するデータなど。

☐ **usage data**: personal data generated by the vehicle, driving habits, location, etc.
- **使用状況データ**: 車両により生成される個人データ、運転習慣、位置など。

111. The EDPB recommends that, as far as possible, and given that there is a risk that the data collected via the telematics-box could be misused to create a precise profile of the driver's movements, raw data regarding driving behaviour should be either processed:
EDPBは、テレマティクス・ボックスを介して収集されるデータが運転者の移動経路を示す正確なプロファイルを作成する目的で悪用されうる点も考慮し、運転行動に関する生データを極力以下のいずれかの方法で取扱うよう勧告する。

☐ inside the vehicle in telematics boxes or in the user's smartphone so that the insurer only accesses the results data (e.g., a score relating to driving habits), not detailed raw data (see section 2.1);
- 保険会社が詳細な生データではなく、結果に関するデータ（例えば運転習慣に関連するスコア）に限定してアクセスするよう、生データは車両に搭載されたテレマティクス・ボックス内又はユーザーのスマートフォン内でのみ取扱う（第2.1節を参照のこと）。

☐ or by the telematics service provider on behalf of the controller (the insurance company) to generate numerical scores that are transferred to the insurance company on a defined basis. In this case, raw data and data directly relating to the identity of the driver must be separated. This means that the telematics service provider receives the real-time data, but does not know the names, licence plates, etc. of the policy holders. On the other hand, the insurer knows the names of policyholders, but only receives the scores and the total kilometres and not the raw data used to produce such scores.
- 又は、管理者（保険会社）の代わりにテレマティクス・サービスのプロバイダーが数値スコアを生成し、所定の時間間隔で保険会社に移転する。この場合、生データと運転者の身元に直接関係するデータは分離しなければならない。これは、テレマティクス・サービスのプロバイダーの側では、リアルタイムデータを取得するものの、保険契約者の氏名、自動車の登録番号などは知らされないことを意味する。他方で、保険会社の側では、保険契約者の氏名はわかっているものの、スコアと走行した合計キロ数のみを受け取り、当該スコアを生成するために利用される生データは受け取らない。

112. Moreover, it has to be noted that if only the mileage is necessary for the performance of the contract, location data shall not be collected.
さらに、契約を履行するために走行距離のみが必要な場合には、位置データを収集してはならない点に注意する必要がある。

3.1.1.3 Retention period
保存期間

113. In the context of data processing taking place for the performance of a contract (i.e. provision of a service), it is important to distinguish between two types of data before defining their respective retention periods:
契約の履行（つまりサービスの提供）のために行われるデータの取扱いの場合には、2種類のデータを区別し、それぞれのデータの保存期間を決定することが重要である。

☐ **commercial and transactional data:** those data can be retained in an active database for the full duration of the contract. At the end of the contract, they can be archived physically (on a

separate medium: DVD, etc.) or logically (by authorisation management) in the event of possible litigation. Thereafter, at the end of the statutory limitation periods, the data shall be deleted or anonymised;

・ **商取引上のデータ：** 契約の全期間中、稼働中のデータベースに保存できる。訴訟になる可能性に備え、契約の終了時に当該データを（DVDなどの別の記憶媒体に）物理的に保管するか、又は（認証アクセス管理システムを備えた）データベースにデータとして保管することができる。保存後、法定の消滅時効期間満了時に、データは消去するか又は匿名化する。

☐ **usage data:** usage data can be classified as raw data and aggregated data. As stated above, if possible, data controllers or processors should not process raw data. If it is necessary, raw data should be kept only as long as they are required to elaborate the aggregated data and to check the validity of that aggregation process. Aggregated data should be kept as long as it is necessary for the provision of the service or otherwise requested by a Union or Member State law.

・**使用状況データ**: 使用状況データは、生データと集約されたデータとに分類できる。上記のように、データ管理者又は処理者は生データを極力取扱うべきではない。生データを取扱う必要がある場合は、生データの保存は集約データを作成し、当該集約過程の有効性を確認するために必要な期間に限定すべきである。集約されたデータは、サービスの提供に必要な期間又はEU法又は加盟国の国内法で要求されている期間に限定して保存するべきである。

3.1.1.4 Information and rights of data subjects
データ主体への情報提供及びデータ主体の権利

114. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. In particular, he or she must be informed of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. In this last case, the EDPB recommends to adopt a pedagogic approach to emphasize the difference between raw data and the score produced on this basis, stressing, when it is the case, that the insurer will only collect the result of the score where appropriate.
データ主体は、個人データが取扱われる前に、GDPR第13条に従い、当該取扱いに関して透明性があり、理解しやすい方法で説明を受ける。特に、その個人データが保存される期間、又は、それが不可能なときは、その期間を決定するために用いられる基準をデータ主体に説明しなければならない。後者の場合、EDPBは、該当する場合は、保険会社は適切な場合にはスコアの結果のみを収集することを強調しつつ、生データと生データを基に作成されるスコアとの違いに焦点を当て、教育的な説明の方法をとるよう勧告する。

115. Where data are not processed inside the vehicle but by a telematics provider on behalf of the controller (the insurance company), the information could usefully mention that, in this case, the provider will not have access to data directly relating to the identity of the driver (such as names, licence plates, etc.). Also, considering the importance of informing data subjects as to the consequences of processing of their personal data and the fact that data subjects should not be taken by surprise by the processing of their personal data, the EDPB recommends that data subject should be informed of the existence of profiling and the consequences of such profiling even if it does not involve any automated decision-making as referred to in art. 22 GDPR.
データが車両内で取扱われず、管理者（保険会社）の代わりにテレマティクス・プロバイダーにより取扱われる場合、当該プロバイダーが、運転者の身元に直接関連するデータ（氏名、自動車登録番号等）にアクセスできない旨の情報を提供することは有益と考えられる。また、自己の個人データが取扱われる場合の結果に関して

データ主体に説明する重要性及びデータ主体が自己の個人データの取扱いに不意を突かれてはならないという事実を考慮し、EDPBは、GDPR第22条で言及されているような自動化された意思決定を伴うものではない場合でも、プロファイリングの存在及び当該プロファイリングの結果に関してデータ主体に説明するよう勧告する。

116. Regarding the right of data subjects, they shall be specifically informed of the available means to exercise his or her right of access, rectification, restriction and erasure. Since raw data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends "that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability[48]."
データ主体は、データ主体の権利に関し、特にアクセス、訂正、制限、及び消去の権利を行使するために利用可能な手段に関して説明を受ける。こうしたケースで収集される生データは、（特定のフォーム又はデータ主体の活動を通じて）データ主体により提供され、かつGDPR第6条(1)(b)（契約の履行）に基づいて取扱われるため、データ主体は、データポータビリティの権利を行使できる。データポータビリティの権利に関するガイドラインで強調されているように、EDPBは、「*データ主体が自己のアクセス権及びデータポータビリティの権利を通じて取得できるデータの種類の差異について、データ管理者が明確に説明するよう*」[48]強く勧告する。

117. The information can be provided when the contract is signed.
情報は、契約締結時に提供することが可能である。

3.1.1.5 Recipient:
取得者:

118. The EDPB recommends that, as far as possible, the vehicle's usage data should be processed directly in telematics boxes, so that the insurer only accesses the results data (e.g. a score), not detailed raw data.
EDPBは、保険会社によるアクセスが詳細な生データではなく結果に関するデータ（例えばスコア）に限定されるように、極力、車両の使用状況データの取扱いを直接テレマティクス・ボックス内で行うよう勧告する。

119. If a telematics service provider collects the data on behalf of the controller (the insurance company) to generate numerical scores, it does not need to know the identity of the driver (such as names, licence plates, etc.) of the policy holders.
テレマティクス・サービスのプロバイダーが数値スコアを生成するために管理者（保険会社）の代わりにデータを収集する場合、当該プロバイダーは保険契約者である運転者の（氏名、自動車登録番号などの）身元を知る必要はない。

3.1.1.6 Security:
安全管理:

120. General recommendations apply. See section 2.7.
一般勧告があてはまる。第2.7節を参照のこと。

[48] Article 29 Working Party, Guidelines on the right to data portability under Regulation 2016/676, WP242 rev.01, endorsed by EDPB, p. 13.
第29条作業部会、「データポータビリティの権利に関するガイドライン」、WP242 rev. 01、EDPB承認版、13頁。

3.1.2 Renting and booking a parking space
駐車場の貸出及び予約

121. The owner of a parking place may want to rent it. For this, he/she lists a spot and sets a price for it on a web application. Then, once the parking spot is listed, the application notifies the owner when a driver wants to book it. The driver can select a destination and check for available parking spots based on multiple criteria. After the approval of the owner, the transaction is confirmed and the service provider handles the payment transaction then uses navigation to drive to the location.
駐車場の所有者がそれを貸し出したい場合がある。当該目的のため、駐車場所有者は、ウェブアプリケーションを使い、自身の所有する駐車場のリストを作成し、各価格を設定する。一旦駐車場の情報がアプリケーション内に掲載されると、アプリケーションが、運転者から予約の申込みが入るたびに当該所有者に通知することになる。運転者は、目的地を選択し、複数の基準に基づいて利用可能な駐車場を確認できる。所有者の承認を得た後に、取引が確認され、サービスプロバイダーが決済取引を扱い、ナビゲーション機能を使ってその場所に誘導する。

3.1.2.1 Legal basis
法的根拠

122. When the data is collected through a publicly available electronic communication, art. 5(3) of the ePrivacy directive applies.
公衆に利用可能な電子通信を介してデータが収集される場合、eプライバシー指令第5条(3)が適用される。

123. Because this is an information society service, art. 5(3) of the ePrivacy directive does not require consent for gaining access to information that is already stored in the vehicle when such a service is explicitly requested by the subscriber.
これは情報社会サービスであるため、eプライバシー指令第5条(3)では、そのようなサービスが加入者により明確に要求される場合に関し、車両に既に保存されている情報へのアクセスを取得する際に同意を得るよう求めていない。

124. For the processing of personal data and only for data necessary for the performance of the contract to which the data subject is party, art. 6(1)(b) GDPR will be the legal basis.
個人データであり、かつデータ主体が当事者である契約の履行に必要なデータに限る取扱いについては、GDPR第6条(1)(b)が当該取扱いの法的根拠になる。

3.1.2.2 Data collected
収集されるデータ

125. Data processed includes the driver contact details (name, email, telephone number, vehicle type (e.g. car, truck, motorcycle), license plate number, parking period, payment details (e.g. credit card info) as well as navigation data.
取扱われるデータは、運転者の連絡先の詳細（氏名、電子メール、電話番号）、車両の種類（乗用車、トラック、オートバイなど）、自動車登録番号、駐車期間、決済方法の詳細（クレジットカード情報など）、及びナビゲーションデータを含む。

3.1.2.3 Retention period
保存期間

126. Data should be retained only as long as it is necessary to fulfil the parking contract or otherwise as provided by Union or Member State law. After that data is either anonymized or deleted.
駐車契約の履行に必要な期間、又はEU法若しくは加盟国の国内法に規定される期間に限定してデータが保存されるべきである。当該期間の経過後、データは匿名化されるか又は消去される。

3.1.2.4 *Information and rights of data subjects*
データ主体への情報提供及びデータ主体の権利

127. Prior to the processing of personal data, the data subject should be informed according to art. 13 GDPR, in a transparent and understandable way.
個人データを取扱う前に、GDPR第13条に従い、当該取扱いに関して透明性があり、理解しやすい方法でデータ主体に説明しなければならない。

128. The data subject should be specifically informed of the available means to exercise his or her right of access, rectification, restriction and erasure. Since the data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends *"that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability"*.
データ主体には、特にアクセス、訂正、制限、及び消去の権利を行使するために利用可能な手段に関して説明しなければならない。こうしたケースで収集されるデータは、（特定のフォーム又はデータ主体の活動を通じて）データ主体により提供され、かつGDPR第6条(1)(b)（契約の履行）に基づいて取扱われるため、データ主体は、データポータビリティの権利を行使できる。データポータビリティの権利に関するガイドラインで強調されているように、EDPBは、「*データ主体が自己のアクセス権及びデータポータビリティの権利を通じて取得できるデータの種類の差異について、データ管理者が明確に説明するよう*」強く勧告する。

3.1.2.5Recipient:
取得者:

129. In principle, only the data controller and the data processor have access to the data.
データにアクセスするのは、原則として、データ管理者とデータ処理者に限られる。

3.1.2.6 *Security:*
安全管理:

130. General recommendations apply. See section 2.7.
一般勧告があてはまる。第2.7節を参照のこと。

3.2 eCall
eCall（緊急通報）

131. In the event of a serious accident in the European Union, the vehicle automatically triggers an eCall to 112, the EU-wide emergency number (see section 1.1 for further details) which allows an ambulance to be sent the place of the accident promptly according to Regulation (EU) 2015/758 of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service, and amending Directive 2007/46/EC (hereinafter - "Regulation (EU) 2015/758").
欧州連合域内で重大な事故を起こした場合、112番サービスを利用したeCall車載システムを装備するための型式認証の要件に関する、及び、指令2007/46/ECを改正する2015年4月29日の規則(EU)2015/758（以下「規則(EU)2015/758」）に従い、当該事故車両はEU域内共通の緊急番号（詳細は第1.1節を参照のこと）である112番へのeCallを自動的に発信し、これにより救急車が事故現場に迅速に派遣されることとなる。

132. Indeed, the eCall generator installed inside the vehicle, which enables transmission via a public mobile wireless communications network initiates an emergency call, which is either triggered automatically by vehicle sensors or manually by the vehicle occupants only in the

event of an accident. In addition to activation of the audio channel, the second event triggered automatically as a result of an accident consists in generating the Minimum Set of Data (MSD) and sending it to the public safety answering point (PSAP).
実際、車両内に搭載されたeCall発信装置は、公衆移動体無線通信ネットワークを介した発信を可能にするものであり、当該緊急通報は、事故が発生した場合に限り車両センサーにより自動的に起動されるか又は車両乗員により手動で起動される。音声の起動に加え、事故の発生を機に、最小データセット（MSD）を生成し、それを緊急通報センター（PSAP）に送信するといった第二の作業が自動的に起こる。

3.2.1 Legal basis
法的根拠

133. Regarding the application of the ePrivacy directive, two provisions have to be considered:
eプライバシー指令の適用に関し、同指令の次の二つの規定を考慮する必要がある。

- art. 9 regarding location data other than traffic data which only applies to electronic communication services;
- 電子通信サービスにのみ適用される交通データ以外の位置データに関する同指令第9条。

- art. 5(3) for the gaining access to information stored in the generator installed inside the vehicle.
- 車両内に設置された発信装置に保存されている情報へのアクセスを取得するための同指令第5条(3)。

134. Despite the fact that, in principle, those provisions require the consent of the data subject, Regulation (EU) 2015/758 constitutes a legal obligation to which the data controller is subject (the data subject has no genuine or free choice and will be unable to refuse the processing of his/her data). Hence, Regulation (EU) 2015/758 overrides the need of the driver's consent for the processing of location data and the MSD. [49]
これらの規定は、原則、データ主体の同意を要件としているが、規則(EU)2015/758は、データ管理者に適用される法的義務を規定する（この場合、データ主体には真の又は自由の選択がなく、また自己のデータの取扱いを拒否できない）。つまり、規則(EU)2015/758は、位置データ及び最小データセット（MSD）の取扱いに関して、運転者の同意を得る要件に優先される[49]。

135. The legal basis of the processing of those data will be compliance with a legal obligation as provided for in art. 6(1)(c) GDPR (i.e., Regulation (EU) 2015/758).
これらのデータの取扱いの法的根拠は、GDPR第6条(1)(c)に規定する法的義務（つまり、規則(EU)2015/758）を遵守するために取扱いが必要な場合となる。

3.2.2 Data collected
収集されるデータ

136. Regulation (EU) 2015/578 provides that data sent by the 112-based eCall in-vehicle system shall include only the minimum information as referred to in the standard EN 15722:2015

[49] It has to be noted that Article 8-1-f of the Council negotiation mandate for the proposal for an "ePrivacy" regulation does provide a specific exemption for eCall as consent is not needed when "it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number '112' or a national emergency number, in accordance with Article 13(3)."
「エンドユーザーが第13条(3)に従い、単一の欧州緊急通報番号『112番』又は国内緊急通報番号のいずれかに緊急通信を行った際、端末機器の位置を検出するために必要である」場合は同意を得る必要がないため、「eプライバシー」規則案・理事会交渉権限付託版の第8条(1)(f)に、eCallに関する特定の適用除外を規定している点に留意しなければならない。

'Intelligent transport systems — eSafety — eCall minimum set of data (MSD)' including:
規則(EU)2015/578は、112番eCall車載システムにより送信されるデータは、標準EN 15722: 2015『高度道路交通システム－eSafety－eCall最小データセット（MSD）』で言及されているように、以下を含む、最小限の情報に限定するよう規定している。

☐ the indication if eCall has been manually or automatically triggered;
- 手動又は自動でeCallが起動されたかどうかの表示。

☐ the vehicle type;
- 車両の型式。

☐ the vehicle identification number (VIN);
- 車両識別番号（VIN）。

☐ the propulsion type of the vehicle;
- 車両の駆動方式。

☐ the timestamp of the initial data message generation within the current eCall incident event;
- 該当のeCall事故事象の範囲内における最初のデータメッセージ生成時のタイムスタンプ。

☐ the last known vehicle latitude and longitude position determined at the latest moment possible before message generation;
- メッセージが生成される可能な限り直前の時点で決定された車両の最後に判明している緯度及び経度。

☐ the vehicle's last known real direction of travel determined at the latest moment possible before message generation (only the last three locations of the vehicle).
- メッセージが生成される可能な限り直前の時点で決定された車両の最後に判明している実際の進行方向（車両の最後の位置3か所のみ）。

3.2.3 Retention period
保存期間

137. Regulation (EU) 2015/758 stipulates that data shall not be retained for longer than is needed for processing emergency situations. Those data shall be completely deleted when they are no longer needed for that purpose. Furthermore, in the internal memory of the eCall system, data shall be automatically and constantly deleted. Only the vehicle's last three positions can be stored, insofar as it is strictly necessary to specify the current position of the vehicle and the direction of travel at the time of the event.
規則(EU)2015/758は、緊急事態の取扱いに必要な期間を超えてデータを保存しないよう規定する。それらのデータは、当該目的で不要になった時点で完全に消去する。加えて、eCallシステムの内部メモリに存在するデータは自動にかつ都度消去する。事故発生時における車両の現在位置及び進行方向を特定するために厳密に必要とされる範囲で、車両の最後の位置3か所のみを保存できる。

3.2.4 Information and rights of data subjects
データ主体への情報提供及びデータ主体の権利

138. Art. 6 of the Regulation (EU) 2015/758 stipulates that manufacturers shall provide clear and complete information on data processing done using the eCall system. This information shall be provided in the owner's manual separately for the 112-based eCall in-vehicle system and any third-party service supported eCall systems prior to the use of the system. It includes:
規則(EU)2015/758の第6条は、メーカーはeCallシステムを使用して行われるデータの取扱いについて、明確で完全な情報を提供するよう規定する。当該情報は、車両

取扱説明書の中で、112番eCall車載システムで取り扱われる情報及び第三者サービスによるeCallシステムで取り扱われる情報と別々に説明され、当該システムを利用する前に提供される。当該情報には以下を含む。

☐ the reference to the legal basis for the processing;
・ 取扱いの法的根拠への言及。

☐ the fact that the 112-based eCall in-vehicle system is activated by default;
・ 112番eCall車載システムが初期設定として起動している事実。

☐ the arrangements for data processing that the 112-based eCall in-vehicle system performs;
・ 112番eCall車載システムが実行するデータの取扱いに関する取決め。

☐ the specific purpose of the eCall processing, which shall be limited to the emergency situations referred to in the first subparagraph of Art. 5(2) Regulation (EU) 2015/758;
・ eCallによる取扱いの特定の目的と、それが、規則(EU)2015/758の第5条(2)の第1号で言及されている緊急事態に限定されること。

☐ the types of data collected and processed and the recipients of that data;
・ 収集され、取扱われるデータの種類及び当該データの取得者。

☐ the time limit for the retention of data in the 112-based eCall in-vehicle system;
・ 112番eCall車載システム内にデータが保存される期限。

☐ the fact that there is no constant tracking of the vehicle;
・ 車両の常時追跡が行われない事実。

☐ the arrangements for exercising data subjects' rights as well as the contact service responsible for handling access requests;
・ データ主体による権利行使の取決め及びデータ主体が自己のデータにアクセスしたい場合の取扱対応窓口。

☐ any necessary additional information regarding traceability, tracking and processing of personal data in relation to the provision of a third-party service (TPS) eCall and/or other added value services, which shall be subject to explicit consent by the owner and in compliance with the GDPR. Particular account shall be taken of the fact that differences may exist between the data processing carried out through the 112-based eCall in-vehicle system and the TPS eCall in-vehicle systems or other added value services.
・ 第三者サービス（TPS）によるeCallサービス及び／又は他の付加価値サービスの提供に関連する個人データの追跡可能性機能、追跡、及び取扱いに必要な追加情報。当該個人データの取扱いについては、データ所有者の明確な同意の取得、及びGDPRへの準拠が要件となる。112番eCall車載システムで実行されるデータ取扱いと、第三者サービス（TPS） eCall車載システム又はその他の付加価値サービスで実行されるデータ取扱いとでは、差異が生じうる事実を特に考慮すること。

139. Furthermore, the service provider shall also provide the data subjects with information in accordance with art. 13 GDPR in a transparent and understandable way. In particular, he or she must be informed of the purposes of the processing for which the personal data are intended as well as the fact that the processing of personal data is based on a legal obligation to which the controller is subject.
さらに、サービスプロバイダーは、GDPR第13条に従い、透明性があり、理解しやすい方法で情報をデータ主体に提供する。特に、データ主体は、個人データの予定されている取扱いの目的、及び管理者の服する法的義務に基づき個人データが取扱われる事実に関して説明を受けなければならない。

140. In addition, taking into account the nature of the processing, the information about the recipients or categories of recipients of the personal data should be clear and the data subjects should be informed that the data are not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.
加えて、取扱いの性質を考慮し、個人データの取得者又は取得者の類型に関する情報は明確なものとし、かつeCallが起動されるまで、112番eCall車載システムの外のいかなる主体にもデータが提供されることはない点をデータ主体に説明するべきである。

141. Regarding rights of data subjects, it has to be noted that since the processing is based on a legal obligation, the right to object and the right to portability will not apply.
データ主体の権利に関し、当該取扱いが法的義務を根拠にしているため、異議を述べる権利及びデータポータビリティの権利が適用されないことに留意する必要がある。

3.2.5 Recipient:
取得者:

142. The data shall not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.
eCallが起動されるまで112番eCall車載システムの外のいかなる主体にもデータが提供されない。

143. When it is triggered (either manually by vehicle occupants or automatically as soon as an in-vehicle sensor detects a serious collision), the eCall system establishes a voice connection with the relevant PSAP and the MSD is sent to the PSAP operator.
eCallが（車両の乗員により手動で又は車載センサーが重大な衝突を検知し次第自動的に）起動されると、eCallシステムは関連する緊急通報センター（PSAP）との音声接続を確立し、最小データセット（MSD）が当該緊急通報センター（PSAP）のオペレーターに送信される。

144. Furthermore, data transmitted via the 112-based eCall in-vehicle system and processed by the PSAPs can be transferred to the emergency service and service partners referred to in Decision No 585/2014/EU only in the event of incidents related to eCalls and under the conditions set out in that Decision and are used exclusively for the attainment of the objectives of that Decision. Data processed by the PSAPs through the 112-based eCall in-vehicle system are not transferred to any other third parties without the explicit prior consent of the data subject.
さらに、112番eCall車載システムを介して移転され、緊急通報センター（PSAP）により取扱われるデータは、eCallに関連する事故が発生した場合にのみ、かつ決定No 585/2014/EUに規定されている条件に基づき、同決定で言及されている救急サービス及び提携サービスに移転でき、また同決定の目的を達成するためにのみ利用される。112番eCall車載システムを介して緊急通報センター（PSAP）により取扱われるデータは、データ主体の明確な事前の同意なく他の第三者に移転されることはない。

3.2.6 Security
安全管理

145. Regulation (EU) 2015/758 stipulates the requirements to incorporate into the eCall system technologies that strengthen the protection of privacy, in order to offer users the appropriate level of protection of privacy, as well as the guarantees needed to prevent surveillance and abusive uses. In addition, manufacturers should ensure that the eCall system based on the number 112, as well as any other system providing an eCall that is

handled by third-party services or an added-value service, are so designed that it is impossible for personal data to be exchanged between those systems.
規則(EU)2015/758は、ユーザーに対し適切な水準のプライバシー保護、並びに監視及び不正使用を防ぐために必要な保証を与える目的でプライバシー保護を強化する技術をeCallシステムに組み込む旨の要件を規定する。さらに、メーカーは、112番eCallシステム、及び第三者サービス又は付加価値サービスが扱う他のeCall提供システムについて、設計上、当該システム間での個人データの交換ができないよう確保するべきである。

146. Regarding PSAPs, Member States should ensure that personal data are protected against misuse, including unlawful access, alteration or loss, and that protocols concerning personal data storage, retention duration, processing and protection are established at the appropriate level and properly observed.
緊急通報センター（PSAP）に関し、加盟国は、個人データが違法なアクセス、改ざん又は紛失などの不正使用から保護されるよう、また個人データの保存、保存期間、取扱い及び保護に関する手順が適切な水準で確立され、適切に監視されるよう確保するべきである。

3.3 Accidentology studies
事故調査

147. Data subjects may voluntarily agree to take part in accidentology studies aimed at better understanding the causes of road accidents and more generally scientific purposes.
データ主体は、交通事故の原因への理解を深めることを目的とする、より一般的には科学的目的のための事故調査に参加することに自発的に同意することがある。

3.3.1 Legal basis
法的根拠

148. When the data are collected through a public electronic communication service, the data controller will have to collect the consent of the data subject for the gaining of access to information that is already stored in the vehicle as provided by art. 5(3) of the ePrivacy directive. Indeed, none of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user.
公衆の電子通信サービスを介してデータが収集される場合、データ管理者が車両に既に保存されている情報へのアクセスを取得するためにはeプライバシー指令第5条(3)に規定されるようにデータ主体の同意を取得する必要がある。こうしたケースでは、同条項に定める適用除外のいずれも適用されない。つまり、当該取扱いは、電子通信ネットワークを介した通信の送信を実行することのみを目的とするものではなく、また、加入者又はユーザーから明確に要求された情報社会サービスに関連するものでもない。

149. Regarding the processing of personal data and taking into account the variety and amount of personal data needed for accidentology studies, the EDPB recommends the processing to be based on the prior consent of the data subject according to art. 6 GDPR. Such prior consent must be provided on a specific form, through which the data subject volunteers to take part to the study and have his or her personal data processed for that purpose. Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g., ticking a box that is not pre-ticked, or configuring the onboard computer to activate a function in the vehicle). Such consent must be provided separately, for specific purposes, may not be bundled with the contract to buy or lease a new car and the consent must be as easily withdrawn as it is given. Withdrawal of consent shall lead to

the processing being stopped. The data shall then be deleted from the active database, or anonymized.
EDPBは、個人データの取扱いに関し、また事故調査に必要な個人データの多様性及び量を考慮し、GDPR第6条に従いデータ主体の事前の同意に基づきデータを取扱うよう勧告する。当該事前の同意は、特定のフォームにより提供されなければならず、当該フォームの提示によりデータ主体は、自発的に当該調査に参加し、当該調査の目的のために自己の個人データが取扱われることに自発的に同意することになる。同意は、（例えば事前にチェックが入っていないチェックボックスにチェックマークを付けるか又は車両の機能を起動するために車載コンピューターを設定するなど）データが取扱われる者による、自由になされ、特定されており、かつ説明を受けたうえでの意思の表示であるものとする。このような同意は、特定の目的ごとに個別に与えられたものでなければならず、また新車を購入又はリースする契約にまとめることはできない。同意は、与える場合と同程度に容易に撤回できなければならない。同意の撤回と同時に取扱いは停止される。この時、データは、稼働中のデータベースから消去されるか、又は匿名化される。

150. Consent required by art. 5(3) of the ePrivacy directive and consent needed as a legal basis for the processing of data can be collected at the same time (for example by checking a box clearly indicating what the data subject is consenting to).
eプライバシー指令第5条(3)により要求される同意及びデータの取扱いの法的根拠として必要とされる同意は（例えばデータ主体が同意しようとしている内容を明確に示すボックスにチェックを入れることにより）、同時に取得することができる。

151. It has to be noted that, depending on the conditions of the processing (nature of the data controller, etc.), another legal basis can be lawfully chosen as long as it does not lower the additional protection provided by art. 5(3) ePrivacy directive (see paragraph 15). If the processing is based on another legal basis such as the performance of a task carried out in the public interest (art. 6(1)(e) GDPR), the EDPB recommends that the data subjects are included in the study on a voluntary basis.
eプライバシー指令第5条(3)に規定される追加的保護を引下げない限り、取扱いの条件（データ管理者の性質など）に応じて、別の法的根拠を適法に選択できる点に注意する必要がある（パラグラフ15を参照のこと）。別の法的根拠、例えば公共の利益において行われる職務の遂行のための取扱い（GDPR第6条(1)(e)）に基づいてデータが取扱われる場合、EDPBは、データ主体の自発的な参加意思に基づき、その者を調査対象に含めるよう勧告する。

3.3.2 Data collected
収集されるデータ

152. The data controller shall only collect personal data that are strictly necessary for the processing.
データ管理者は、取扱いに厳密に必要とされる個人データに限定し収集する。

153. There are two types of data to be considered:
考慮すべきデータは次の2種類存在する。

☐ **data relating to participants and vehicles**;
・ **参加者及び車両に関連するデータ、**

☐ **technical data from vehicles**(instantaneous speed, etc.).
・ **車両から得られる技術データ**（瞬間速度など）。

154. Scientific research linked to accidentology justifies the collection of the instantaneous speed, including by legal persons who do not administer a public service in the strict sense.

事故調査に関連する科学的調査は、厳密な意味で公共サービスを運営していない法人によるものも含め、瞬間速度データの収集を正当化する。

155. Indeed, as noted above, the EDPB considers that instantaneous speed collected in the context of an accidentology study is not offence-related data by destination (i.e., it is not being collected for the purpose of investigating or prosecuting an offence), which justifies its collection by legal persons who do not administer a public service in the strict sense.
上記のように、EDPBは、事故調査に関連して収集される瞬間速度データは、取扱いの目的上、犯罪行為関連データではない（つまり犯罪の捜査又は訴追の目的で収集されていない）ため、厳密な意味で公共サービスを運営していない法人による当該データの収集は正当化されると考える。

3.3.3 Retention period
保存期間

156. It is important to distinguish between two types of data. First, the data relating to participants and vehicles can be retained for the duration of the study. Second, the technical data from vehicles should be retained for as short as possible for the purpose. In this regard, five years from the end date of the study appears to be a reasonable period. At the end of that period, the data shall be deleted or anonymized.
2種類のデータを区別することが重要である。第一に、参加者及び車両に関連するデータは調査の全期間保存できる。第二に、事故調査目的での車両から得られる技術データの保存期間は極力短くするべきである。この点に関し、調査の終了日から5年間が妥当な期間だと思われる。当該期間の終わりに、データを消去するか又は匿名化すること。

3.3.4 Information and rights of data subjects
データ主体への情報提供及びデータ主体の権利

157. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. In particular, in the case of collecting instantaneous speed, the data subjects should be specifically informed of the data collection. Since the data processing is based on consent, the data subject must be specifically informed of the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Moreover, because the data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(a) GDPR (consent), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends “that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability.” Consequently, the data controller should provide an easy way to withdraw his consent, freely and at any time, as well as develop tools to be able to answer data portability requests.
データ主体は、個人データが取扱われる前に、GDPR第13条に従い、当該取扱いに関して透明性があり、理解しやすい方法で説明を受ける。特に、瞬間速度データを収集する場合、当該データ収集に関してデータ主体に具体的に説明を行うべきである。データの取扱いが同意を根拠とするため、データ主体は、その撤回前の同意に基づく取扱いの適法性に影響を与えることなく、いつでも同意を撤回する権利が存在する旨の説明を明確に受けなければならない。さらに、こうしたケースで収集されるデータは、（特定のフォーム又はデータ主体の活動を通じて）データ主体により提供され、かつGDPR第6条(1)(a)（同意）に基づいて取扱われるため、データ主体は、データポータビリティの権利を行使できる。データポータビリティの権利に関するガイドラインで強調されているように、EDPBは、「*データ主体が自己のア*

クセス権及びデータポータビリティの権利を通じて取得できるデータの種類の差異について、データ管理者が明確に説明するよう」強く勧告する。結果として、データ管理者は、データ主体が自己の同意をいつでも自由に撤回できるような簡単な方法を提供し、またデータポータビリティの要求に応じることを可能にするようなツールを開発するべきである。

158. That information can be given upon signing the form to agree to take part in the accidentology study.
当該情報は、事故調査に参加することに同意するためのフォームに署名する際に提供することが可能である。

3.3.5 Recipient
取得者

159. In principle, only the data controller and the data processor have access to the data.
データにアクセスできるのは原則としてデータ管理者及びデータ処理者に限られる。

3.3.6 Security
安全管理

160. As noted above, the security measures put in place shall be adapted to the level of data sensitivity. For instance, if instantaneous speed (or any other data related to criminal convictions and offences) is collected as part of the accidentology study, the EDPB strongly recommends putting in place strong security measures, such as:
上記のように、講じられる安全管理措置は、データの機微性の水準に合わせて調整すること。例えば、事故調査の一環として瞬間速度データ（又は有罪判決及び犯罪行為に関連する他のデータ）が収集される場合、EDPBは、次のような強固な安全管理措置を講ずるよう強く勧告する。

☐ implementing pseudonymisation measures (e.g., secret-key hashing of data like the surname/first name of the data subject and the serial number);
- 仮名化措置（例えば、データ主体の姓／名及びシリアル番号などのデータの鍵付きハッシング）の導入。

☐ storing data relating to instantaneous speed and to location in separate databases (e.g., using a state-of-the-art encryption mechanism with distinct keys and approval mechanisms);
- 瞬間速度と位置に関連するデータを（例えば、それぞれ異なる鍵及び承認メカニズムを備えた最先端の暗号化メカニズムを利用して）別々のデータベースに保存すること。

☐ and/or deleting location data as soon as the reference event or sequence is qualified (e.g., the type of road, day/night), and the storage of directly-identifying data in a separate database that can only be accessed by a small number of people.
- 及び／又は基準となる事象又は一連の事象（道路の種類、昼／夜など）が限定され次第、位置データを消去し、直接識別可能なデータを少人数のみアクセスできる別なデータベースに保存すること。

3.4 Tackle auto theft
自動車盗難対策

161. Data subjects may wish, in the case of theft, to attempt to find their vehicle using location. Using location data is limited to the strict needs of the investigation and to the case assessment by the competent legal authorities.
盗難に遭遇した場合、データ主体が位置データを使って自身の車を見つけたいと希望する場合がある。位置データの使用は、法的に権限のある当局による捜査及び事

案評価に厳密に必要とされる範囲に限定される。

3.4.1 Legal basis
法的根拠

162. When the data is collected through a publicly available electronic communication service, art. 5(3) of the ePrivacy directive applies.
公衆に利用可能な電子通信サービスを介してデータが収集される場合には、eプライバシー指令第5条(3)が適用される。

163. Because this is an information society service, art. 5(3) of the ePrivacy directive does not require consent for gaining access to information that is already stored in the vehicle when such a service is explicitly requested by the subscriber.
これは情報社会サービスであるため、eプライバシー指令第5条(3)では、そのようなサービスが加入者により明確に要求される場合に関し、車両に既に保存されている情報へのアクセスを取得する際に同意を得るよう求めていない。

164. Regarding the processing of personal data, the legal basis for processing the location data will be the consent of the vehicle's owner, or, if applicable, the performance of a contract (only for data necessary for the performance of the contract to which the vehicle's owner is party).
個人データの取扱いに関し、位置データを取扱うための法的根拠は、車両の所有者による同意、又は該当する場合は、契約の履行（ただし、車両の所有者が当事者である契約を履行するために必要なデータの取扱いに限る）となるであろう。

165. Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g. ticking a box that is not pre-ticked, or configuring the on-board computer to activate a function in the vehicle). Freedom to give consent involves the option of withdrawing consent at any time, of which the data subject should be expressly informed. Withdrawal of consent shall lead to the processing being stopped. The data should then be deleted from the active database, anonymized, or archived.
同意は、（例えば事前にチェックが入っていないチェックボックスにチェックマークを付けるか又は車両の機能を起動するために車載コンピューターを設定するなど）データが取扱われる者による、自由になされ、特定されており、かつ説明を受けたうえでの意思の表示であるものとする。同意の自由が存在するには、同意をいつでも撤回する選択肢がデータ主体に与えられ、そのことがデータ主体に明確に説明されなければならない。同意の撤回と同時に取扱いは停止される。この時、データは稼働中のデータベースから消去されるか、匿名化されるか、又は保管されなければならない。

3.4.2 Data collected
収集されるデータ

166. Location data can only be transmitted as of the declaration of theft, and cannot be collected continuously the rest of the time.
位置データは、盗難の被害届時以降のものに限り移転できるものとし、それ以外の期間中に継続的に収集することは許されない。

3.4.3 Retention period
保存期間

167. Location data can only be retained for the period during which the case is assessed by the competent legal authorities, or until the end of a procedure to dispel doubt that does not end with confirmation of the theft of the vehicle.
位置データは、法的に権限のある当局により事案が評価されている期間中、又は車

両の盗難確認では終了しない嫌疑を払拭する手続が終了するまでの期間中に限り保存できる。

3.4.4 Information of the data subjects
データ主体への情報

168. Prior to the processing of personal data, the data subject should be informed according to art. 13 GDPR, in a transparent and understandable way. More specifically, the EDPB recommends that the data controller emphasizes that there is no constant tracking of the vehicle and that location data can only be collected and transmitted as of the declaration of theft. Moreover, the controller must provide the data subject with information relating to the fact that only approved officers of the remote-surveillance platform and legally approved authorities have access to the data.
個人データを取扱う前に、GDPR第13条に従い、当該取扱いに関して透明性があり、理解しやすい方法でデータ主体に説明しなければならない。より具体的には、EDPBは、車両が常時追跡されていないこと、盗難の届出時以降の位置データに限定して収集し、移転することが可能であることをデータ管理者が強調するよう勧告する。さらに、管理者は、遠隔監視プラットフォーム・サービス提供事業者の承認された職員及び法的に承認された当局のみがデータにアクセスできるという事実に関する情報をデータ主体に提供しなければならない。

169. Regarding the rights of the data subjects, when the data processing is based on consent, the data subject should be specifically informed of the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Besides, when the data collected in this context are provided by them (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(a) (consent) or art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends "that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability".
データ主体の権利に関し、データの取扱いが同意に基づく場合、データ主体は、その撤回前の同意に基づく取扱いの適法性に影響を与えることなく、いつでも同意を撤回する権利が存在する旨の説明を明確に受けるべきである。加えて、こうしたケースで収集されるデータは、（特定のフォーム又はデータ主体の活動を通じて）データ主体により提供され、かつGDPR第6条(1)(a)（同意）又は同第6条(1) (b)（契約の履行）に基づいて取扱われるため、データ主体は、データポータビリティの権利を行使できる。データポータビリティの権利に関するガイドラインで強調されているように、EDPBは、「*データ主体が自己のアクセス権及びデータポータビリティの権利を通じて取得できるデータの種類の差異について、データ管理者が明確に説明するよう*」強く勧告する。

170. Consequently, the data controller should provide an easy way to withdraw his consent (only when consent is the legal basis), freely and at any time, as well as develop tools to be able to answer data portability requests.
結果として、データ管理者は、（同意が法的根拠である場合には）データ主体が自己の同意をいつでも自由に撤回できるような簡単な方法を提供し、またデータポータビリティの要求に応じることを可能にするようなツールを開発するべきである。

171. The information can be provided when the contract is signed.
当該情報は、契約に署名する際に提供することが可能である。

3.4.5 Recipients

取得者

172. In the event of a theft declaration, location data can be passed on the (i) approved officers of the remote-surveillance platform, and (ii) to the legally approved authorities.
盗難の届出が行われた場合、(i)遠隔監視プラットフォーム・サービス提供事業者の承認された職員、及び(ii)法的に承認された当局に位置データを引き渡すことができる。

3.4.6 Security
安全管理

173. General recommendations apply. See section 2.7
一般勧告があてはまる。第2.7節を参照のこと。