

Насоки



**Насоки 1/2020 относно обработването на лични данни
при свързаните превозни средства и приложенията,
свързани с мобилността**

Версия 2.0

Приети на 9 март 2021 г.

История на версиите

Версия 2.0	9 март 2021 г.	Приемане на насоките след обществена консултация
Версия 1.0.	28 януари 2020 г.	Приемане на насоките за обществена консултация

1	Въведение	4
1.1	Публикации по темата	5
1.2	Приложимо право	7
1.3	Обхват	9
1.4	Определения.....	12
1.5	Рискове за неприкосновеността на личния живот и защитата на данните.....	15
2	ОБЩИ ПРЕПОРЪКИ	18
2.1	Категории данни	18
2.2	Цели	20
2.3	Относимост и свеждане на данните до минимум.....	20
2.4	Защита на данните на етапа на проектирането и по подразбиране	20
2.5	Информация.....	24
2.6	Права на субекта на данни	26
2.7	Сигурност	27
2.8	Предаване на лични данни на трети страни	28
2.9	Предаване на лични данни извън ЕС/ЕИП	29
2.10	Използване на бордови технологии за безжична локална мрежа	30
3	ПРАКТИЧЕСКИ КАЗУСИ	30
3.1	Предоставяне на услуга от трета страна.....	30
3.2	Система за автоматични спешни повиквания.....	34
3.3	Проучвания на произшествия.....	38
3.4	Борба с кражбите на автомобили	40

като взе предвид член 70, параграф 1, буква д) от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (наричан по-нататък „ОРЗД“),

като взе предвид Споразумението за ЕИП, и по-специално приложение XI и Протокол 37 към него, изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.¹,

като взе предвид член 12 и член 22 от своя Правилник за дейността,

ПРИЕ СЛЕДНИТЕ НАСОКИ:

1 ВЪВЕДЕНИЕ

1. Символът на икономиката на ХХ век — автомобилът, е един от продуктите за масово потребление, повлиял на обществото като цяло. Често свързвани с понятието за свобода, автомобилите обикновено са считани за нещо повече от транспортно средство. Действително те представляват лично пространство, в което хората могат да се ползват от известна автономност при вземането на решения, без да срещат каквато и да било външна намеса. В днешно време, с навлизането на свързаните превозни средства в стандартното производство, това виждане вече не отговаря на реалността. Свързаността на автомобилите бързо се разпространява от луксозните модели и първокласните марки до моделите с голям дял на пазарите на средния потребител, а превозните средства се превръщат в центрове за масиви от данни. Не само превозните средства, но и водачите и пътниците стават все по-свързани. Всъщност много модели, пуснати на пазара през последните няколко години, включват датчици и свързано бордово оборудване, чрез които може да се събират и записват данни, наред с другото, за експлоатационните показатели на двигателя, начина на управление на автомобила, посетенията места и евентуално дори движенията на очите на водача, неговия пулс или биометрични данни за целите единствено на идентифицирането на физическо лице².
2. Това обработване на данни се извършва в сложна екосистема, която не се ограничава до традиционните участници в автомобилната промишленост, но се оформя и от появата на нови участници от сектора на цифровата икономика. Тези нови участници може да предлагат информационно-развлекателни услуги, като онлайн музика, информация за състоянието на пътя и движението по пътищата, или да предоставят системи, и услуги за подпомагане на управлението на превозното средство, като софтуер за автопилот, актуализации на състоянието на превозното средство, застраховане, основано на използването, или динамично картографиране. Освен това, тъй като превозните средства са свързани чрез електронни съобщителни мрежи, ръководителите на пътната инфраструктура и операторите на далекосъобщителни

¹ Позоваването на „държави членки“ в настоящия документ следва да се разбира като позоваване на „държавите — членки на ЕИП“.

² Инфо-графика „Данните и свързаният автомобил“ от форума „Бъдещето на неприкосновеността на личния живот“: https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

системи, участващи в този процес, също играят важна роля по отношение на потенциалните операции по обработване на личните данни на водачите и пътниците.

3. Освен това, свързаните превозни средства генерират все по-голямо количество данни, голяма част от които могат да се считат за лични данни, понеже ще се отнасят до водачите или пътниците. Дори ако данните, събрани от свързан автомобил, не са пряко свързани с име, а с технически аспекти и характеристики на превозното средство, те ще се отнасят до водача или пътниците на автомобила. Например данните, свързани със стила на управление на превозното средство или изминатото разстояние, данните, свързани с износването на частите на превозното средство, данните за местонахождението или данните, събрани от камерите, може да се отнасят до поведението на водача, както и до информация за други хора, които биха могли да бъдат в превозното средство, или за субекти на данни, които преминават покрай него. Такива технически данни се генерират от физическо лице и позволяват неговата пряка или непряка идентификация от страна на администратора на лични данни или от друго лице. Превозното средство може да се разглежда като крайно устройство, което може да се използва от различни ползватели. Следователно, както при персоналния компютър, потенциалното използване от повече ползватели не засяга личния характер на данните.
4. През 2016 г. Международната автомобилна федерация (МАФ) проведе кампания в цяла Европа, наречена „Моята кола, моите данни“, за да получи отзиви за това какво мислят европейците за свързаните автомобили³. Въпреки че показва големия интерес на водачите към свързаността, тя също така разкрива бдителността, която трябва да се проявява по отношение на използването на данните, генерирани от превозните средства, както и значението на спазването на законодателството за защита на личните данни. Следователно предизвикателството е всяка заинтересована страна да включи защитата на личните данни още на етапа на проектирането на продукта и да гарантира, че ползвателите на автомобили се радват на прозрачност, и контрол по отношение на своите данни в съответствие със съображение 78 от ОРЗД. Такъв подход спомага за укрепване на доверието на ползвателите и съответно за дългосрочното развитие на тези технологии.

1.1 Публикации по темата

5. През последното десетилетие свързаните превозни средства се превърнаха в съществена тема за регулаторите, като през последните няколко години се наблюдава значително увеличение на броя им. В тази връзка са публикувани различни трудове на национално и международно равнище, които са свързани със сигурността и неприкосновеността на личния живот при използването на свързаните превозни средства. С тези разпоредби и инициативи се цели съществуващите рамки в областта на защитата на данните и неприкосновеността на личния живот да се допълнят със специфични за сектора правила или да се предоставят насоки на специалистите.

1.1.1 Инициативи на европейско и на международно равнище

6. От 31 март 2018 г. насам бордовата система за автоматични спешни повиквания , основаваща се на телефон 112, е задължителна за всички нови типове моторни превозни средства от категория M1 и N1 (леки пътнически автомобили и лекотоварни

³ Кампания „Моята кола, моите данни“: <http://www.mycarmydata.eu/>

превозни средства)⁴.⁵ Още през 2006 г. Работната група по член 29 прие работен документ относно последиците за защитата на данните и неприкосновеността на личния живот при инициативата⁶. В допълнение, както беше обсъдено по-рано, през октомври 2017 г. Работната група по член 29 също така прие становище относно обработването на лични данни при съвместните интелигентни транспортни системи (СИТС).

7. През януари 2017 г. Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) публикува проучване, съсредоточено върху киберсигурността и устойчивостта на интелигентните автомобили, в което са изброени чувствителните предимства, както и съответните заплахи, рискове, смекчаващи фактори и възможни мерки за сигурност, които да се прилагат⁷. През септември 2017 г. Международната конференция на комисарите по защита на личните данни и неприкосновеността на личния живот прие резолюция относно свързаните превозни средства⁸. И накрая, през април 2018 г. Международната работна група за защита на данните в телекомуникациите също прие работен документ относно свързаните превозни средства⁹.

1.1.2 Национални инициативи на членовете на Европейския комитет по защита на данните (ЕКЗД)

8. През януари 2016 г. Конференцията на германските органи по защита на данните на федерално равнище и равнище провинции и Германската асоциация на автомобилната промишленост публикува обща декларация относно принципите на защита на данните при свързани и несвързани превозни средства¹⁰. През август 2017 г. Центърът за свързани и автономни превозни средства на Обединеното кралство публикува насоки, в които са изложени принципите за киберсигурност за свързани и автоматизирани превозни средства, с цел да се повиши осведомеността по този въпрос в сектора на автомобилостроенето¹¹. През октомври 2017 г. френският орган за защита на данните, Националната комисия по информатика и свободи (CNIL), публикува пакет за привеждане в съответствие на свързани автомобили с цел да предостави помощ на заинтересованите страни относно начините за интегриране на защитата на данните на етапа на проектирането и по подразбиране, което ще позволи на субектите на данни да имат ефективен контрол върху своите данни¹².

⁴ Оперативно съвместимата в целия ЕС на системата за автоматични спешни повиквания:

https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en

⁵ Решение № 585/2014/EU на Европейския парламент и на Съвета от 15 май 2014 г. за въвеждането на оперативно съвместимата в целия Съюз услуга eCall (текст от значение за ЕИП): <https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32014D0585>

⁶ Работен документ относно последиците за защитата на данните и неприкосновеността на личния живот при инициативата eCall: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf

⁷ Киберсигурност и устойчивост на интелигентните автомобили:

<https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>

⁸ Резолюция относно защитата на данните при автоматизираните и свързаните превозни средства:

https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf

⁹ Работен документ относно свързаните превозни средства: <https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/>

¹⁰ Аспекти на защитата на данните при използването на свързани и несвързани превозни средства:

https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf

¹¹ Принципи за киберсигурност за свързаните и автоматизираните превозни средства:

<https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles>

¹² Пакет за привеждане в съответствие за отговорно използване на данните при свързани автомобили:

<https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data>

1.2 Приложимо право

9. Приложимата правна уредба на ЕС е ОРЗД. Регламентът се прилага във всички случаи, когато обработването на данни при свързани превозни средства включва обработване на лични данни на физически лица.
10. В допълнение към ОРЗД с Директива 2002/58/ЕО, преразгледана с Директива 2009/136/ЕО (наричана по-нататък „Директивата за правото на неприкосновеност на личния живот и електронни комуникации“), **се установява специален стандарт за всички участници, които желаят да съхраняват или да осъществяват достъп до информация, съхранявана в крайното оборудване на абонат или ползвател в Европейското икономическо пространство (ЕИП).**
11. Всъщност, ако повечето от разпоредбите на Директивата за правото на неприкосновеност на личния живот и електронни комуникации (член 6, член 9 и т.н.) се прилагат само за доставчиците на публично достъпни електронни съобщителни услуги и доставчиците на обществени съобщителни мрежи, то член 5, параграф 3 от същата директива е обща разпоредба. Тя се прилага не само за електронни съобщителни услуги, но и за всеки субект, частноправен или публичноправен, който поставя информация в крайно оборудване или я чете от такова оборудване, без значение какво е естеството на данните, които се съхраняват или до които се осъществява достъп.
12. Що се отнася до понятието „*крайно оборудване*“, определение за него е дадено в Директива 2008/63/ЕО¹³. В член 1, буква а) крайното оборудване е определено като „*устройство, предназначено за пряко или непряко свързване към интерфейс на обществена далекосъобщителна мрежа за пренасяне, обработка и приемане на информация; и в двата случая, пряко или непряко, свързването може да бъде осъществено чрез жици, оптични влакна или електромагнитен път; свързването е непряко, ако устройството е поставено между крайното устройство и интерфейса на обществената мрежа; б) оборудване за спътникови наземни станции*“.
13. В резултат на това, при условие че горепосочените критерии са изпълнени, свързаното превозно средство и устройството, свързано с него, следва да се считат за „*крайно оборудване*“ (точно като компютър, смартфон или интелигентен телевизор) и разпоредбите на член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации се прилагат, когато е уместно.
14. Както ЕКЗД подчерта в своето Становище 5/2019 относно взаимодействието между Директивата за правото на неприкосновеност на личния живот и електронни комуникации и ОРЗД¹⁴, в член 5, параграф 3 от посочената директива се предвижда, че по принцип се изисква предварително съгласие за съхраняването на информация или за получаването на достъп до информация, която вече се съхранява в крайното оборудване на абоната или ползвателя освен в случаите на изключения от този принцип, посочени в точка 17 по-долу. Доколкото информацията, съхранявана в устройството на крайния ползвател, представлява лични данни, член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни

¹³ Директива 2008/63/ЕО на Комисията от 20 юни 2008 г. относно конкуренцията на пазарите на крайни далекосъобщителни устройства (текст от значение за ЕИП) (кодифицирана версия): <https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX%3A32008L0063>

¹⁴ Европейски комитет по защита на данните, Становище 5/2019 относно взаимодействието между Директивата за правото на неприкосновеност на личния живот и електронни комуникации и ОРЗД, по-специално що се отнася до компетентността, задачите и правомощията на органите за защита на данните, прието на 12 март 2019 г. (наричано по-нататък „Становище 5/2019“), точка 40.

комуникации има предимство пред член 6 от ОРЗД по отношение на дейността на съхраняване или на получаване на достъп до тази информация¹⁵. Последващото обработване на лични данни след горепосочените операции по обработване, включително обработване на лични данни, получени чрез достъп до информация в крайното оборудване, също трябва да има правно основание съгласно член 6 от ОРЗД, за да бъде законосъобразно¹⁶.

15. Тъй като когато иска съгласие за съхраняване или за получаване на достъп до информация съгласно член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, администраторът ще трябва да информира субекта на данни за всички цели на обработването — включително всяко обработване след горепосочените операции (т.е. „последващо обработване“) — съгласие по член 6 от ОРЗД по принцип би било най-подходящото правно основание, което да обхваща обработването на лични данни след такива операции (доколкото целта на следващото обработване е обхваната от съгласието на субекта на данни, вж. точки 53—54 по-долу). Следователно, съгласието вероятно ще представлява правното основание както за съхраняването, така и за получаването на достъп до вече съхранявана информация, както и за последващото обработване на лични данни¹⁷. На практика при оценката на съответствието с член 6 от ОРЗД следва да се има предвид, че обработването като цяло включва специфични дейности, по отношение на които законодателните органи на ЕС са се постарали да предоставят допълнителна защита¹⁸. Освен това при определяне на подходящото законово основание администраторите трябва да отчетат ефекта върху правата на субектите на данни, за да се спази принципът на добросъвестност¹⁹. Изводът е, че администраторите не могат да се позовават на член 6 от ОРЗД с цел намаляване на допълнителната защита, предвидена в член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.
16. ЕКЗД припомня, че понятието за съгласие в Директивата за правото на неприкосновеност на личния живот и електронни комуникации остава същото като понятието за съгласие в ОРЗД и трябва да отговаря на всички изисквания, предвидени в член 4, точка 11 и член 7 от ОРЗД.
17. Въпреки това, макар че съгласието е правилото, в член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации се допуска случаи на съхраняване на информация или получаване на достъп до информация, която вече е съхранявана в крайното оборудване, да бъдат освободени от изискването за информирано съгласие, ако удовлетворяват един от следните критерии:
-) **освобождение 1:** с единствена цел осъществяване на предаването на съобщение по електронна съобщителна мрежа;
 -) **освобождение 2:** когато това е строго необходимо, за да може доставчикът да предостави услуга на информационното общество, изрично поискана от абоната или ползвателя.

¹⁵ Пак там, точка 40.

¹⁶ Пак там, точка 41.

¹⁷ Съгласието, което се изисква по член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, и съгласието, необходимо като правно основание за обработването на данни (член 6 от ОРЗД) за една и съща конкретна цел, могат да бъдат получени едновременно (например чрез поставяне на отметка в поле, където ясно се посочва с какво се съгласява субектът на данни).

¹⁸ Становище 5/2019, точка 41.

¹⁹ Европейски комитет по защита на данните, Насоки 2/2019 относно обработката на лични данни съгласно член 6, параграф 1, буква б) от Общия регламент относно защита на данните при предоставянето на онлайн услуги на субектите на данни, версия 2.0, 8 октомври 2019 г., точка 1.

18. В тези случаи обработването на лични данни, включително лични данни, получени чрез достъп до информация в крайното оборудване, се основава на едно от правните основания, предвидени в член 6 от ОРЗД. Така например съгласие не се изисква, когато обработването на данни е необходимо за целите на предоставянето на GPS навигационно обслужване, поискано от субекта на данни, когато такова обслужване може да бъде определено като услуги на информационното общество.

1.3 Обхват

19. ЕКЗД би желал да изтъкне, че настоящите насоки са предназначени да улеснят привеждането в съответствие на обработването на лични данни, извършвано от широк кръг заинтересовани страни, които работят в тази среда. Те обаче нямат за цел да обхванат всички възможни случаи на използване или да предоставят указания за всяка възможна конкретна ситуация.

20. Обхватът на настоящия документ е съсредоточен, по-специално, върху обработването на лични данни във връзка с използването за непрофесионални цели на свързани превозни средства от страна на субектите на данни: например водачи, пътници, собственици на превозни средства, други участници в пътното движение и т.н. По-конкретно в него са разгледани личните данни: i) които се обработват в превозното средство; ii) които се обменят между превозното средство и личните устройства, свързани с него (например смартфона на ползвателя); или iii) които се събират на място в превозното средство и се препращат за по-нататъшно обработване на външни субекти (например производители на превозни средства, ръководители на инфраструктури, застрахователни дружества, автосервиси).

21. В настоящия документ определението за свързано превозно средство трябва да се разбира в широкия смисъл. Свързаното превозно средство може да се определи като превозно средство, оборудвано с множество електронни блокове за управление (ЕБУ), които са свързани заедно чрез бордова мрежа, както и инструменти, които му позволяват да обменя информация с други устройства в превозното средство и извън него. Сами по себе си данните могат да бъдат обменяни между превозното средство и личните устройства, свързани с него, например чрез възможност за отразяване на мобилните приложения в устройството с информационни и развлекателни функции на арматурното табло на автомобила. Също така разработването на самостоятелни мобилни приложения, т.е. независими от превозното средство (например разчитащи единствено на използването на смартфон), които са в помощ на водачите, е включено в обхвата на настоящия документ, тъй като те допринасят за капацитета за свързаност на превозното средство, въпреки че може на практика да не разчитат на обмена на данни със самото превозно средство. Приложенията за свързани превозни средства са много на брой и разнообразни, и могат да включват²⁰:

22. *управление на мобилността*: функции, които позволяват на водачите да достигат местоназначението бързо и по разходно ефективен начин, като осигуряват своевременна информация относно GPS навигация, потенциално опасни условия на околната среда (например- заледени пътища), претоварвания на движението или пътни строително-ремонтни работи, помощ за намиране на място за паркиране или в гаража, оптимизиране на разхода на гориво или пътни такси;

23. *управление на превозното средство*: функции, които са предназначени да подпомагат водачите за намаляване на оперативните разходи и подобряване на

²⁰ Стратегия на Прайсуотърхаузкупърс, 2014 г. „In the fast lane. The bright future of connected cars“ („В бързата лента. Светлото бъдеще на свързаните автомобили“):
https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf

удобството при използване на средството, като известяване за състоянието на превозното средство и напомняния за техническо обслужване, прехвърляне на данни за използването (например за услуги за ремонт на превозното средство), съобразени с клиента застраховки от типа „плащане според ползването на автомобила“/„плащане според поведението при управление на автомобила“, отдалечени операции (например- отоплителна система) или конфигуриране на профили (например- положение на седалките);

24. *безопасност на движението по пътищата*: функции, които предупреждават водача за външни опасности и вътрешни мерки за реагиране, например защита от сблъсък, предупреждения за опасност, предупреждения за излизане от лентата, засичане на сънливост на водача, спешни повиквания или „черни кутии“ за разследване на катастрофа (устройство, записващо данни за събитията);
25. *развлечение*: функции, предоставящи информация и развлечения за водача и пътниците, като например интерфейси за смартфон (телефонни обаждания с функция „свободни ръце“, генериране на текстово от гласово съобщение), зони с безжична локална мрежа, музика, видеосъдържание, интернет, социални медии, мобилен офис или услуги за интелигентни сгради;
26. *подпомагане на водача*: функции, свързани с частично или напълно автоматизирано управление на превозното средство, като например оперативна помощ или автопилот при натоварено движение, при паркиране или при управление на превозното средство на магистрала;
27. *благосъстояние*: функции за наблюдение на удобството на водача, способността и пригодността му да управлява превозното средство, като например засичане на умора или медицинска помощ.
28. Съответно превозните средства могат да бъдат или да не бъдат свързани по подразбиране и лични данни могат да бъдат събирани по няколко начина, включително чрез: i) датчици в превозното средство; ii) телематични модули; или iii) мобилни приложения (например такива, до които се осъществява достъп от устройство, принадлежащо на водача). За да попадат в обхвата на настоящия документ, мобилните приложения трябва да са свързани със средата на управление на превозното средство. Пример за обхванати приложения са приложенията за GPS навигация. Приложенията обаче, чиито функции служат само да предлагат на водачите места, представляващи интерес (ресторанти, исторически паметници и др.), попадат извън обхвата на настоящите насоки.
29. Голяма част от данните, които се генерират от свързано превозно средство, се отнасят до физическо лице, което е идентифицирано или което може да бъде идентифицирано, и следователно представляват лични данни. Информацията например включва данни, по които лицата могат да бъдат идентифицирани пряко (например пълните данни за самоличността на водача), както и такива, по които могат да бъдат идентифицирани косвено, като подробности за пропътуваните маршрути, данни за използването на превозното средство (например такива, свързани със стила на управление на превозното средство или с изминатото разстояние), или техническите данни на превозното средство (свързани с износването на частите на превозното средство), които чрез съпоставяне с други сведения и по-специално идентификационния номер на превозното средство могат да бъдат отнесени до физическо лице. Личните данни в свързаните превозни средства могат да включват също така метаданни, като например състоянието на техническо обслужване на превозното средство. С други думи, всички данни, които могат да бъдат свързани с физическо лице, попадат в обхвата на настоящия документ.

30. Екосистемата на свързаните превозни средства обхваща широк спектър от заинтересовани страни. В нея по-конкретно се включват традиционните участници от автомобилната промишленост, както и новопоявяващите се от цифровия сектор. Поради тази причина настоящите насоки са ориентирани към производителите на превозни средства и на оборудване, и доставчиците за сектора на автомобилостроенето, автосервизите, дистрибуторите на автомобили, доставчиците на обслужване на превозни средства, управителите на автопаркове, застрахователните дружества, предлагачи застраховки за моторни превозни средства, доставчиците на развлекателни услуги, операторите на далекосъобщителни услуги, ръководителите на пътна инфраструктура, и публичните органи, както и субектите на данни. ЕКЗД подчертава, че категориите субекти на данни ще бъдат различни при различните услуги (например водачи, собственици, пътници и т.н.). Това е неизчерпателен списък, тъй като екосистемата се отнася до широк спектър от услуги, включително такива, за които се изисква пряко удостоверяване на автентичността или идентификация, както и услуги, за които те не се изискват.
31. Някои видове обработване на данни, извършвани от физическите лица в превозното средство, попадат в обхвата на критерия „в хода на чисто лични или домашни занимания“ и съответно не са обхванати от ОРЗД²¹. По-конкретно това се отнася до използването на лични данни в превозните средства единствено от онези субекти на данни, които са предоставили такива данни в арматурното табло на превозното средство. ЕКЗД обаче припомня, че съгласно съображение 18 от ОРЗД регламентът „се прилага за администратори или обработващи лични данни, които осигуряват средствата за обработване на лични данни при такива лични дейности или дейности в рамките на домакинството“.

1.3.1 Случаи извън обхвата на настоящия документ

32. Работодателите, предоставящи служебни автомобили на членовете на персонала си, може да желаят да наблюдават действията на своите служители (например, за да гарантират безопасността на служителя, стоките или превозното средство, да разпределят ресурси, да проследяват и да начисляват такса за услуга или да проверяват работното време). Обработването на данни, извършвано от работодателите в тази връзка, повдига конкретни съображения, свързани с трудовата заетост, които може да са регламентирани в трудовото право на национално равнище, което не може да бъде подробно представено в настоящите насоки²².
33. Въпреки че обработването на данни при използване на търговските превозни средства за професионални цели (като обществен транспорт) и за споделен транспорт и решения за „мобилност като услуга“ , може да повдигне определени съображения, които не са обхванати от настоящите общи насоки, много от принципите и препоръките, изложени тук, са приложими и за тези видове обработване.
34. Тъй като свързаните превозни средства са системи, работещи чрез радиоизлъчване, те подлежат на пасивно проследяване, като например проследяване чрез WLAN или Bluetooth. В този смисъл те не се различават от други свързани устройства и попадат в приложното поле на Директивата за правото на неприкосновеност на личния живот и електронни комуникации, която понастоящем е предмет на преразглеждане. Следователно, това изключва и широкомащабното проследяване на оборудвани с

²¹ Вж. член 2, параграф 2, буква в) от ОРЗД.

²² Работната група за защита на личните данни по член 29 е разгледала тези въпроси в своето Становище 2/2017 относно обработването на данни на работното място (РД 249): https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

безжични локални мрежи (WLAN) превозни средства²³ от гъста мрежа от странични наблюдатели, които използват общи услуги за местонахождение чрез смартфони. Тези странични наблюдатели редовно докладват всички видими WLAN мрежи на централните сървъри. Тъй като вградените безжични локални мрежи могат да се считат за вторичен идентификатор на превозното средство²⁴, това поражда риск от системно текущо събиране на данни за пълни профили на движенията на превозните средства.

35. Превозните средства все по-често се оборудват с устройства за записване на изображения (например- системи от камери за улесняване на паркирането или автомобилни цифрови видеорегистратори). Тъй като това е свързано с въпроса за заснемането на обществени места, което изисква оценка на съответната законодателна рамка, специфична за всяка отделна държава членка, този вид обработване на данни е извън обхвата на настоящите насоки.
36. Обработването на данни в основата на съвместните интелигентни транспортни системи (СИТС) — както са определени в Директива 2010/40/ЕС²⁵, е разгледано в отделно становище на Работната група за защита на личните данни по член 29²⁶. Макар че определението на концепцията за СИТС в директивата не съдържа технически спецификации, в своето становище Работната група за защита на личните данни по член 29 се е съсредоточила върху комуникациите с малък обем, т.е. такива, които не изискват намесата на мрежов оператор. По-конкретно, тя предоставя анализ на конкретни случаи на използване, свързани с първоначалното внедряване на системите, и поема ангажимент да оцени на по-късен етап новите въпроси, които несъмнено ще бъдат повдигнати, когато се използва по-високо равнище на автоматизация. Тъй като последствията за защитата на данните при използването на СИТС са много специфични (безпрецедентен обем на данните за местонахождение, непрекъснато предаване на лични данни, обмен на данни между превозните средства и други съоръжения на пътните инфраструктури и т.н.), и понеже те все още се обсъждат на европейско равнище, обработването на лични данни в този смисъл не е обхванато в настоящите насоки.
37. И накрая, настоящият документ няма за цел да се разгледат всички възможни повдигнати проблеми и въпроси, отнасящи се до свързаните превозни средства, и поради това не може да се счита за изчерпателен.

1.4 Определения

38. Понятието **обработване** на лични данни обхваща всяка операция, извършвана с лични данни, като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез

²³ Вж. за подробна информация: <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 и Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings (Идентифициране на превозните средства въз основа на вторичен идентификатор на превозното средство — анализ и измервания в производството), VEHICULAR 2017, Шеста международна конференция по въпросите на напредъка при автомобилните системи, технологии и приложения, Ница, Франция, 23—27 юли, 2017 г., стр. 32—37.

²⁵ Директива 2010/40/ЕС на Европейския парламент и на Съвета от 7 юли 2020 г. относно рамката за внедряване на интелигентните транспортни системи в областта на автомобилния транспорт и за интерфейси с останалите видове транспорт: <https://eur-lex.europa.eu/legal-content/bg/TXT/PDF/?uri=CELEX:32010L0040>

²⁶ Работна група за защита на личните данни по член 29 — Становище 3/2017 относно обработването на лични данни в контекста на съвместните интелигентни транспортни системи (СИТС): http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171

предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване и др.²⁷.

39. **Субектът на данни** е физическото лице, за което се отнасят данните, обхванати от обработването. При свързаните превозни средства това може например да бъде водачът (основен или случаен), пътникът или собственикът на превозното средство²⁸.
40. **Администраторът на лични данни** е лицето, което определя целите и средствата на обработването, което се извършва в свързаните превозни средства²⁹. Администратори на лични данни могат да бъдат доставчиците на услуги, които обработват данни от превозното средство, за да изпратят на водача информация за пътното движение, съобщения за екологосъобразно управление на превозното средство или предупреждения във връзка с функционирането на превозното средство, застрахователни дружества, предлагащи полици от типа „*плащане според ползването на автомобила*“, или производители на превозни средства, събиращи информация относно износването на частите на превозното средство с цел подобряване на неговото качество. Съгласно член 26 от ОРЗД двама или повече администратори могат съвместно да определят целите и средствата на обработването и съответно да се считат за съвместни администратори. В този случай те трябва да определят по прозрачен начин съответните си задължения, по-специално що се отнася до упражняването на правата на субектите на данни и предоставянето на информацията, посочена в членове 13 и 14 от ОРЗД.
41. **Обработващ лични данни** е всяко лице, което обработва лични данни за и от името на администратора на лични данни³⁰. Обработващият данни събира и обработва лични данни по нареждане на администратора, без да ги използва за свои собствени цели. За илюстрация, в редица случаи производителите на оборудване и доставчиците за сектора на автомобилостроенето може да обработват данни от името на производителите на превозни средства (което не означава, че те не могат да бъдат администратори на лични данни, обработвани за други цели). Освен изискването обработващите лични данни да прилагат подходящи технически и организационни мерки с цел да гарантират равнище на сигурност, което е съобразено с рисковете, в член 28 от ОРЗД са определени и техните задълженията.
42. **Получател** означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не³¹. За илюстрация, търговски партньор на доставчика на услуги, който получава от доставчика лични данни, генерирани от превозното средство, е получател на лични данни. Независимо дали изпълняват функцията на нов администратор на данни, или на обработващ лични данни, те трябва да спазват всички задължения, наложени от ОРЗД.
43. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“³²; обработването на тези данни от посочените публични органи трябва да отговаря на приложимите правила за защита на данните съобразно целите на обработването. Така например, правоприлагащите органи са

²⁷ Вж. член 4, точка 2 от ОРЗД.

²⁸ Вж. член 4, точка 1 от ОРЗД.

²⁹ Вж. член 4, точка 7 от ОРЗД и Европейски комитет по защита на данните, Насоки 7/2020 относно концепциите за администратор и обработващ лични данни в ОРЗД (наричани по-нататък „Насоки 7/2020“).

³⁰ Вж. член 4, точка 8 от ОРЗД и Насоки 7/2020.

³¹ Вж. член 4, точка 9 от ОРЗД и Насоки 7/2020.

³² Вж. член 4, точка 9 и съображение 31 от ОРЗД.

упълномощени трети страни, когато изискват лични данни като част от разследване в съответствие с правото на Европейския съюз или правото на държава членка.

1.5 Рискове за неприкосновеността на личния живот и защитата на данните

44. Работната група по член 29 вече е изразила няколко опасения относно системите на интернет на предметите, които могат да се прилагат и за свързаните превозни средства³³. Въпросите, свързани със сигурността и контрола на данните, обработвани във връзка с интернет на предметите, са още по-чувствителни в случаите на свързаните превозни средства, тъй като това води до опасения относно пътната безопасност — и може да повлияе на физическата неприкосновеност на водача — в среда, традиционно възприемана като изолирана и защитена от външни смущения.
45. Също така свързаните превозни средства пораждаат значителни опасения относно защитата на данните и неприкосновеността на личния живот по отношение на обработването на данни за местонахождение, тъй като все по-вмешателският характер на това обработване може да окаже натиск върху настоящите възможности за запазване на анонимност. ЕКЗД иска да постави особен акцент и да повиши осведомеността на заинтересованите страни относно факта, че използването на технологии за откриване на местонахождението изисква прилагането на специфични гаранции, за да се предотвратят наблюдението на физически лица и злоупотребата с данните.

1.5.1 Липса на контрол и информационна асиметрия

46. Водачите и пътниците на превозни средства невинаги могат да бъдат адекватно информирани за обработването на данни, което се извършва в свързано превозно средство или чрез него. Информацията може да бъде предоставена само на собственика на превозното средство, който може да не е водачът, а може и да не бъде предоставена своевременно. Следователно, съществува риск от недостатъчно предлагане на функции или опции, за да се извършва контролът, необходим на засегнатите физически лица да упражняват своите права на защита на данните и неприкосновеност на личния живот. Този въпрос е важен, тъй като по време на експлоатационния си срок превозните средства може да принадлежат на повече от един собственик в случаи на продажба или отдаване под наем.
47. Също така комуникацията в рамките на превозното средство може да се задейства автоматично, както и по подразбиране, без човек да е наясно с това. За ползвателя ще бъде изключително трудно да контролира потока от данни при липсата на възможност за ефективен контрол на начините за взаимодействие между превозното средство и неговото свързано оборудване. Още по-трудно ще бъде да се контролира последващото използване на данните, а оттам и да се предотврати потенциалното използване за други цели.

1.5.2 Качество на съгласието на ползвателя

48. ЕКЗД подчертава, че когато обработването на данни се основава на съгласие, всички елементи на валидно съгласие трябва да бъдат изпълнени, което означава, че съгласието трябва да бъде свободно изразено, конкретно и информирано и да представлява недвусмислено указание за волята на субекта на данни съгласно тълкуването в насоките на ЕКЗД относно съгласието³⁴. Администраторите на лични данни трябва да обърнат специално внимание на условията за получаване на валидно съгласие от различни участници, като собственици или ползватели на автомобили. Това съгласие трябва да се предоставя отделно, за конкретни цели и не може да бъде

³³ Работна група по член 29 — Становище 8/2014 относно последните разработки в сферата на интернет на нещата: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_bg.pdf

³⁴ Европейски комитет по защита на данните, Насоки 5/2020 относно съгласието в съответствие с Регламент 2016/679, версия 1.1, 4 май 2020 г. (наричани по-нататък „Насоки 5/2020“).

включвано в договора за закупуване или наемане на нов автомобил. Съгласието трябва да може да се оттегля толкова лесно, колкото е дадено.

49. Същото трябва да се прилага, когато е необходимо съгласието да отговаря на разпоредбите на Директивата за правото на неприкосновеност на личния живот и електронни комуникации, например, ако се съхранява информация или се получава достъп до информация, която вече се съхранява в превозното средство, както се изисква в някои случаи, обхванати от член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Всъщност, както беше посочено по-горе, съгласието трябва да се тълкува в светлината на ОРЗД.
50. В много случаи е възможно ползвателят да не знае за извършваното обработване на данни в неговото превозно средство. Подобна липса на информация представлява сериозна пречка за доказването на валидно съгласие съгласно ОРЗД, тъй като съгласието трябва да бъде информирано. При такива обстоятелства съответното обработване на данни не може да се основава на съгласието като правно основание.
51. В сферата на свързаните превозни средства може да се окаже трудно да се прилагат класическите механизми, използвани за получаване на съгласието на физически лица, което води до съгласие с „ниско качество“, основано на липса на информация, или до фактическа невъзможност за предоставяне на прецизирано съгласие в съответствие с изразените от физическите лица предпочитания. На практика може да бъде трудно да се получи и съгласието на водачи и пътници, които не са свързани със собственика на превозното средство, в случай на употребявани, наети/отдадени под наем или взети назаем превозни средства.
52. Когато Директивата за правото на неприкосновеност на личния живот и електронни комуникации не изисква съгласието на субекта на данни, администраторът все пак носи отговорността да избере правното основание съгласно член 6 от ОРЗД, което е най-подходящо за случая в съответствие с целите на обработването на лични данни.

1.5.3 По-нататъшно обработване на лични данни

53. Когато данните се събират въз основа на съгласие съгласно изискванията на член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации или на едно от изключенията по член 5, параграф 3 и впоследствие бъдат обработени в съответствие с член 6 от ОРЗД, те може да бъдат обработвани по-нататък само, ако администраторът на лични данни поиска допълнително съгласие за тази друга цел или ако може да докаже, че обработването се основава на правото на Съюза или на държава членка с оглед гарантиране на целите, посочени в член 23, параграф 1 от ОРЗД³⁵. ЕКЗД счита, че в такива случаи не е възможно по-нататъшно обработване въз основа на проверка за съвместимост съгласно член 6, параграф 4 от ОРЗД, тъй като това би подкопало стандарта за защита на данните, предвиден в Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Всъщност, когато в съответствие с Директивата за правото на неприкосновеност на личния живот и електронни комуникации се изисква съгласие, то трябва да бъде конкретно и информирано, което означава, че субектите на данни трябва да са наясно с всяка цел на обработването на данните и да имат право да отказват конкретни видове обработване³⁶. Да се счита, че е възможно по-нататъшно обработване въз основа на заложената в член 6, параграф 4 от ОРЗД проверка за

³⁵ Вж. също Европейски комитет по защита на данните, Насоки 10/2020 относно ограниченията по член 23 от ОРЗД.

³⁶ Насоки 5/2020, вж. раздели 3.2 и 3.3.

съвместимост, би означавало да се заобиколи изискванията за съгласие, заложен в действащата директива.

54. ЕКЗД припомня, че с първоначалното съгласие не се узаконява нито един случай на по-нататъшно обработване, тъй като съгласието трябва да бъде информирано и конкретно, за да бъде валидно.
55. Така например данните във връзка с измерване от разстояние, които се събират по време на използване на превозното средство за целите на техническото обслужване, не може да бъдат разкривани на застрахователните дружества без съгласието на ползвателите с цел създаване на профили на водачи, на които да се предлагат застрахователни полици, в зависимост от извършена преценка на поведението при управление на превозното средство.
56. Освен това данните, събирани от свързани превозни средства, може да бъдат обработвани от правоприлагащите органи с цел констатиране на нарушения, свързани с превишена скорост, или други нарушения, ако и когато са изпълнени конкретните условия в Директивата относно правоприлагането в областта на защитата на данните. В този случай такива данни ще се считат за свързани с присъди и престъпления при условията, определени в член 10 от ОРЗД и всяко приложимо национално законодателство. Производителите може да предоставят на правоприлагащите органи такива данни, ако конкретните условия за такова обработване са изпълнени. ЕКЗД посочва, че обработването на лични данни единствено с цел изпълнение на искания, отправени от правоприлагащите органи, не представлява конкретна, изрично указана и легитимна цел по смисъла на член 5, параграф 1, буква б) от ОРЗД. Когато правоприлагащите органи са упълномощени по закон, те могат да бъдат трети страни по смисъла на член 4, точка 10 от ОРЗД, като в този случай производителите ще имат право да им предоставят всички данни, с които разполагат, при спазване на съответната правна рамка във всяка държава членка.

1.5.4 Прекомерно събиране на данни

57. Поради все по-големия брой датчици, разполагани в свързаните превозни средства, съществува много висок риск от прекомерно събиране на данни в сравнение с това, което е необходимо за постигане на целта.
58. Разработването на нови функции и по-конкретно такива, базирани на алгоритми за машинно обучение, може да изисква голямо количество данни, събирани през дълъг период от време.

1.5.5 Сигурност на личните данни

59. Многообразието от функции, услуги и интерфейси (например за интернет, USB, радиочестотна идентификация, безжична локална мрежа), предлагани чрез свързани превозни средства, увеличава повърхността, уязвима за атаки, и съответно броя на потенциалните слаби места, чрез които личните данни могат да бъдат компрометирани. За разлика от повечето устройства, базирани на интернет на предметите, свързаните превозни средства са критични системи, при които нарушаването на сигурността може да застраши живота на ползвателите и хората наоколо. Поради това се засилва значението на справянето с риска от хакери, опитващи се да използват слабите места на свързаните превозни средства.
60. Освен това личните данни, съхранявани в превозни средства и/или на външни местонахождения (например в инфраструктури за изчисления в облак), трябва да бъдат адекватно защитени от неразрешен достъп. Например, по време на техническото обслужване превозното средство трябва да бъде предадено на техник, който ще поиска достъп до някои от техническите данни на превозното средство.

Въпреки че техникът трябва да има достъп до техническите данни, съществува възможност той да се опита да получи достъп до всички данни, съхранявани в превозното средство.

2 ОБЩИ ПРЕПОРЪКИ

61. За да се намалят установените по-горе рискове за субектите на данни, производителите на превозни средства и оборудване, доставчиците на услуги или всяка друга заинтересована страна, която може да действа като администратор или обработващ лични данни по отношение на свързани превозни средства, трябва да следват изброените по-долу общи препоръки.

2.1 Категории данни

62. Както беше отбелязано във въведението, повечето данни относно свързани превозни средства ще се считат за лични данни, доколкото е възможно да бъдат свързани с едно или повече физически лица, които може да бъдат идентифицирани. Това включва технически данни относно движенията на превозното средство (например- скорост, изминато разстояние), както и относно състоянието на превозното средство (например- температура на охлаждащата течност на двигателя, обороти на двигателя, налягане в гумите). Някои данни, генерирани от свързани превозни средства, също може да се нуждаят от специално внимание предвид тяхната чувствителност и/или потенциално въздействие върху правата и интересите на субектите на данни. Понастоящем ЕКЗД определи три категории лични данни, които се нуждаят от специално внимание от страна на производителите на превозни средства и оборудване, доставчиците на услуги и други администратори на лични данни: данни за местонахождение, биометрични данни (и всяка специална категория данни, определена в член 9 от ОРЗД) и данни, които могат да разкрият престъпления или нарушения на правилата за движение по пътищата.

2.1.1 Данни за местонахождение

63. Когато събират лични данни, производителите на превозни средства и оборудване, доставчиците на услуги и други администратори на лични данни следва да имат предвид, че данните за местонахождение са особено показателни за житейските навици на субектите на данни. Извършените пътувания са много характерни, тъй като позволяват да се направи извод за местоработата и местоживеенето, както и за центровете на интересите на водача (свободното време) и евентуално може да разкрият чувствителна информация, например религия чрез мястото на богослужение, или сексуална ориентация чрез посетените места. Съответно, производителят на превозни средства и оборудване, доставчикът на услуги и друг администратор на лични данни трябва да бъдат особено бдителни да не събират данни за местонахождение, освен ако това е абсолютно необходимо за целите на обработването. Така например, когато обработването се състои в установяване на движението на превозното средство, жироскопът е достатъчен, за да изпълни тази функция, без да е необходимо да се събират данни за местонахождение.

64. Като цяло събирането на данни за местонахождение зависи също от спазването на следните принципи:

Z подходяща конфигурация на честотата на достъп до събираните данни за местонахождение и на степента на тяхната детайлност с оглед на целта на обработването. Например, приложение за метеорологични условия не следва да има достъп до местонахождението на превозното средство всяка секунда, дори със съгласието на субекта на данни;

- Z предоставяне на точна информация относно целта на обработването (например съхранява ли се история на местонахождението? Ако е така, с каква цел?);
- Z когато обработването се основава на съгласие, получаване на валидно (свободно изразено, конкретно и информирано) съгласие, което се различава от общите условия за продажба или използване, например на бордовия компютър;
- Z активиране на местонахождението само когато ползвателят стартира функция, която изисква местонахождението на превозното средство да бъде известно, а не по подразбиране и непрекъснато при запалване на автомобила;
- Z информиране на ползвателя, че установяването на местонахождението е активирано, по-специално чрез използване на икони (например стрелка, която се движи през екрана);
- Z възможност за деактивиране на местонахождението по всяко време;
- Z определяне на ограничен период на съхранение.

2.1.2 Биометрични данни

65. При свързаните превозни средства биометрични данни, използвани за целите единствено на идентифицирането на физическо лице, може да се обработват по смисъла на член 9 от ОРЗД и изключенията на национално равнище, наред с другото, за да се позволи достъп до превозно средство, да се установи самоличността на водача/собственика и/или да се позволи достъп до настройките и предпочитанията на профила на водача. Когато се обмисля използването на биометрични данни, осигуряването на субекта на данни на пълен контрол върху неговите данни включва, от една страна, предвиждането на алтернатива, различна от биометрични данни (например използване на физически ключ или код), без допълнителни ограничения (т.е. използването на биометрични данни не трябва да бъде задължително), и от друга страна, съхраняване и сравняване на биометричния образец в криптирана форма само на вътрешно равнище, като биометричните данни не се обработват от външен терминал за четене/сравняване.
66. В случай на обработване на биометричните данни³⁷ е важно да се гарантира, че решението за биометрична проверка е достатъчно надеждно, по-специално чрез спазване на следните принципи:
- Z използваното решение за биометрична проверка (например процентите на фалшива положителна и отрицателна идентификация) бива адаптирано към равнището на сигурност, което е заложено за прилагане на необходимия контрол на достъпа;
 - Z използваното решение за биометрична проверка се основава на датчик, който е устойчив на атаки (като използването на плосък печат за разпознаване на пръстови отпечатьци);
 - Z броят на опитите за установяване на самоличността е ограничен;
 - Z биометричният образец/модел се съхранява в превозното средство в криптирана форма, като се използват алгоритъм за криптиране и управление на ключове, които отговарят на съвременното технологично равнище;
 - Z необработените данни, използвани за съставяне на биометричния образец и за удостоверяване на автентичността на ползвателя, се обработват в реално време, без изобщо да се съхраняват, дори на място в превозното средство.

³⁷ Принципът за забрана, определен в член 9, параграф 1 от ОРЗД, се отнася само до „биометрични данни за целите единствено на идентифицирането на физическо лице“.

2.1.3 Данни, разкриващи престъпления или други нарушения

67. За да се обработват данни, които се отнасят до потенциални престъпления по смисъла на член 10 от ОРЗД, ЕКЗД препоръчва да се прибегне до обработване на данните на място, при което субектът на данни има пълен контрол върху въпросното обработване (вж. дискусиата относно обработването на място в раздел 2.4). Действително — освен при някои изключения (вж. практическия казус относно проучванията на произшествия, представен по-долу в раздел 3.3) — външното обработване на данни, разкриващи престъпления или други нарушения, е забранено. Следователно в зависимост от чувствителността на данните трябва да бъдат въведени строги мерки за сигурност като описаните в раздел 2.7, за да се осигури защита срещу незаконния достъп, изменянето и заличаването на тези данни.
68. На практика някои категории лични данни от свързани превозни средства могат да разкрият, че е извършено или се извършва престъпление или друго нарушение („данни, свързани с престъпления“) и поради това подлежат на специални ограничения (например данни, сочещи, че превозното средство е настъпило разделителната ивица, моментната скорост на превозното средство, съчетана с точни данни за местонахождение). По-специално, в случай че такива данни ще бъдат обработвани от компетентните национални органи за целите на наказателно разследване и преследване, ще се прилагат гаранциите, предвидени в член 10 от ОРЗД.

2.2 Цели

69. Личните данни може да бъдат обработвани за най-различни цели във връзка със свързани превозни средства, включително безопасност на водача, застраховане, ефективен превоз, развлекателни или информационни услуги. В съответствие с ОРЗД администраторите на лични данни трябва да гарантират, че събират лични данни за „конкретни, изрично указани и легитимни“ цели, че не ги обработват по-нататък по начин, несъвместим с тези цели, и че имат валидно правно основание за обработването, както се изисква в член 5 от ОРЗД. Някои конкретни примери за цели, които могат да бъдат преследвани от администраторите на лични данни, извършващи дейност, свързана със свързаните превозни средства, са обсъдени в част III от настоящите насоки заедно с конкретни препоръки за всеки вид обработване.

2.3 Относимост и свеждане на данните до минимум

70. За да спазват принципа на свеждане на данните до минимум³⁸, производителите на превозни средства и оборудване, доставчиците на услуги и други администратори на лични данни следва да обръщат специално внимание на категориите данни от свързано превозно средство, от които се нуждаят, тъй като те трябва да събират само лични данни, които са относими и необходими за обработването. Например, данните за местонахождение нарушават неприкосновеността в особена степен и могат да разкрият много житейски навици на субектите на данни. Съответно участниците от промишлеността следва да бъдат особено бдителни да не събират данни за местонахождение, освен ако това е абсолютно необходимо за целите на обработването (вж. дискусиата относно данните за местонахождение в раздел 2.1 по-горе).

2.4 Защита на данните на етапа на проектирането и по подразбиране

71. Предвид обема и разнообразието на личните данни, генерирани от свързани превозни средства, ЕКЗД отбелязва, че администраторите на лични данни трябва да гарантират, че технологиите, внедрени в свързаните превозни средства, са конфигурирани така, че да се защита неприкосновеността на личния живот на физическите лица чрез прилагане

³⁸ Член 5, параграф 1, буква в) от ОРЗД.

на задълженията за защита на данните на етапа на проектирането и по подразбиране съгласно изискванията на член 25 от ОРЗД. Технологиите следва да бъдат проектирани така, че събирането на лични данни да се сведе до минимум, да се осигурят настройки по подразбиране за защита на неприкосновеността на личния живот и да се гарантира, че субектите на данни са добре информирани, и имат възможност лесно да внасят изменения в конфигурации, свързани с техните лични данни. Конкретни насоки за това как производителите и доставчиците на услуги могат да спазват принципа на защита на данните на етапа на проектирането и по подразбиране могат да бъдат от полза за промишлеността и доставчиците на приложения — трети страни.

72. Някои общи практики, описани по-долу, също могат да помогнат за намаляване на рисковете за правата и свободите на физическите лица, засягащи свързаните превозни средства³⁹.

2.4.1 Обработване на лични данни на място

73. По принцип производителите на превозни средства и оборудване, доставчиците на услуги и други администратори на лични данни следва, когато е възможно, да използват процеси, които не включват лични данни или предаване на лични данни извън превозното средство (т.е. данните се обработват вътрешно). Характерът на свързаните превозни средства обаче крие рискове, като например възможността за атаки от външни участници срещу обработването на място или изтичане на вътрешни данни при продажба на части от превозното средство. Съответно следва да се обърне достатъчно внимание и да се вземат предвид подходящи мерки за сигурност, за да се гарантира, че обработването на място си остава такова. Този сценарий предлага предимството да се гарантира на ползвателя едноличен и пълен контрол върху личните му данни и сам по себе си той представлява по-малък риск за неприкосновеността на личния живот „на етапа на проектирането“, особено като се забранява всякакво обработване на данни от заинтересованите страни без знанието на субекта на данни. Той също така дава възможност за обработване на чувствителни данни, като биометрични данни или данни, свързани с престъпления или други нарушения, както и подробни данни за местонахождение, които иначе биха били предмет на по-строги правила (вж. по-долу). По подобен начин сценарият представлява по-малък риск за киберсигурността и при него има малко закъснение, което го прави особено подходящ за функциите за подпомагане на автоматизираното управление на превозното средство. Някои примери за този вид решения може да включват:

- Z приложения за екологосъобразно управление на превозното средство, при които се обработват данни в превозното средство, за да може на екрана на бордовия компютър да се показват съвети в реално време за екологосъобразно управление;
- Z приложения, които включват предаване на лични данни към устройство, например смартфон, под пълен контрол на ползвателя (например чрез Bluetooth или безжична локална мрежа) и при които данните на превозното средство не се предават на доставчиците на приложенията или производителите на превозните средства; това би включвало например свързване на смартфони, за да се използват дисплеят на автомобила, мултимедийните системи, микрофон (или други датчици) за телефонни разговори и т.н., доколкото събраните данни остават под контрола на субекта на данни и се използват изключително за предоставяне на услугата, която е поискал;

³⁹ Вж. също Европейски комитет по защита на данните, [Насоки № 4/2019 относно член 25, Защита на данните на етапа на проектирането и по подразбиране](#), версия 2.0, приети на 20 октомври 2020 г. (наричани по-нататък „Насоки 4/2019“).

- Z приложения за повишаване на безопасността в превозното средство, например такива, които осигуряват звукови сигнали или вибрации на волана, когато водачът изпреварва автомобил, без да даде мигач, или се отклонява от разделителните ивици, или приложения, които предоставят предупреждения за състоянието на превозното средство (например предупреждение за износване на спирачните накладки);
- Z приложения за отключване, запалване и/или активиране на определени команди за превозното средство, като се използват биометричните данни на водача, които се съхраняват в превозното средство (например модели на лице или глас или данни за пръстови отпечатащи).
74. Приложения като горепосочените включват обработване, извършвано с цел провеждане на чисто лични занимания от физическо лице (т.е. без предаване на лични данни към администратор или обработващ лични данни). Следователно в съответствие с член 2, параграф 2 от ОРЗД **тези приложения не попадат в обхвата на ОРЗД.**
75. Макар обаче ОРЗД да не се прилага за обработването на лични данни от физическо лице в хода на чисто лични или домашни занимания, той се прилага за администратори или обработващи лични данни, които осигуряват средствата за обработване на лични данни при такива лични или домашни занимания (производители на автомобили, доставчик на услуги и др.) в съответствие със съображение 18 от ОРЗД. Следователно, когато действат като администратор или обработващ лични данни, те трябва да разработят сигурно автомобилно приложение при надлежно зачитане на принципа на неприкосновеност на личния живот на етапа на проектирането и по подразбиране. Във всички случаи съгласно съображение 78 от ОРЗД „ *[п]ри разработването, проектирането, подбора и използването на приложения, услуги и продукти, които се основават на обработване на лични данни или обработват лични данни, за да изпълнят функцията си, производителите на продукти, услуги и приложения следва да бъдат насърчавани да вземат предвид правото на защита на личните данни при разработването и проектирането на такива продукти, услуги и приложения и като отчитат надлежно достиженията на техническия прогрес, да се уверят, че администраторите и обработващите лични данни са в състояние да изпълняват своите задължения за защита на данните*“⁴⁰. От една страна, това ще подобри разработването на ориентирани към ползвателите услуги, а от друга страна, ще улесни и осигури всяко по-нататъшно използване в бъдеще, което може да попадне отново в приложното поле на ОРЗД. По-конкретно ЕКЗД препоръчва разработването на сигурна платформа за автомобилни приложения, която да е физически разделена от съответните функции за безопасност на автомобила, така че достъпът до данните за автомобила да не зависи от ненужни външни възможности за достъп чрез използването на облачни технологии.
76. Производителите на автомобили и доставчиците на услуги следва, когато е възможно, да обмислят обработването на данни на място, за да се намалят потенциалните рискове от изчисленията в облак, както е подчертано в становището на Работната група по член 29 относно изчисленията в облак⁴¹.
77. По принцип ползвателите следва да могат да контролират начина, по който техните данни се събират и обработват в превозното средство:

⁴⁰ За повече препоръки относно неприкосновеността на личния живот на етапа на проектирането и по подразбиране вж. Насоки 4/2019.

⁴¹ Работна група по член 29 — Становище 05/2012 относно изчисленията в облак:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_bg.pdf

- Z информацията относно обработването трябва да бъде предоставена на езика на водача (ръководство, настройки и т.н.);
- Z ЕКЗД препоръчва по подразбиране да се обработват само данни, които са строго необходими за функционирането на превозното средство. Субектите на данни следва да имат възможност да активират или деактивират обработването на данни за всички други цели и администратори/обработващи лични данни и да имат възможност да заличат съответните данни, като вземат предвид целта и правното основание на обработването на данните;
- Z данните не следва да се предават на трети страни (т.е. единствено ползвателят има достъп до данните);
- Z данните следва да се пазят само докато са необходими за предоставянето на услугата или съгласно изискванията на правото на Съюза или на държава членка;
- Z субектите на данни следва да могат да заличават окончателно всички лични данни, преди превозните средства да бъдат пуснати за продажба;
- Z субектите на данни следва, когато е възможно, да имат пряк достъп до данните, генерирани чрез тези приложения.

78. И накрая, макар че невинаги е възможно да се прибегне до обработване на данни на място за всеки случай на използване, в много случаи може да се въведе „смесено обработване“. Например при застраховането, основано на използването, личните данни относно поведението при управление на превозното средство (например силата, упражнявана върху спирачния педал, изминатия пробег и т.н.) могат да бъдат обработвани в рамките на превозното средство или от доставчика на телематични услуги от името на застрахователното дружество (администратора на лични данни), за да се генерират цифрови показатели, които се предават на застрахователното дружество на определен период (например ежемесечно). По този начин застрахователното дружество не получава достъп до необработените данни относно поведението, а само до общите показатели, които са резултат от обработването. Това гарантира, че принципите на свеждане на данните до минимум са изпълнени на етапа на проектирането. Това означава и че ползвателите трябва да имат възможност да упражняват правото си, когато данните се съхраняват от други страни: например ползвателят следва да има възможност да заличава данни, съхранявани в системите на автосервиз или автокъща, съгласно условията на член 17 от ОРЗД.

2.4.2 Анонимизация и псевдонимизация

79. Ако се предвижда предаване на лични данни извън превозното средство, преди да бъдат предадени, следва да се обмисли тяхното анонимизиране. При анонимизиране администраторът трябва да вземе предвид цялото обработване, което потенциално може да доведе до повторна идентификация на данни, като например предаване на анонимизирани на място данни. ЕКЗД припомня, че принципите на защита на данните не се прилагат по отношение на анонимна информация, т.е. информация, която не е свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, или по отношение на лични данни, които са анонимизирани по такъв начин, че субектът на данни да не може или вече да не може да бъде идентифициран⁴². След като даден набор от данни наистина бъде анонимизиран и физическите лица вече не могат да бъдат идентифицирани, европейското право за защита на данните вече не се прилага. В резултат на това анонимизацията, когато е

⁴² Член 4, точка 1 и съображение 26 от ОРЗД.

уместно, може да бъде добра стратегия за запазване на предимствата и за намаляване на рисковете във връзка със свързаните превозни средства.

80. Както е подробно описано в Становището на Работната група по член 29 относно техническите способности за анонимизиране, за да се постигне анонимизация на данните, могат да се използват различни методи, които понякога се съчетават⁴³.
81. Други технически способности, като псевдонимизацията⁴⁴, могат да помогнат за свеждане до минимум на рисковете, генерирани от обработването на данните, като се има предвид, че в повечето случаи за постигане на целта на обработването не са необходими данни, които могат да бъдат идентифицирани. Ако псевдонимизацията е подсилена с гаранции за сигурност, тя подобрява защитата на личните данни, като намалява риска от злоупотреба. Псевдонимизацията е обратима, за разлика от анонимизацията, и псевдонимизираните данни се считат за лични данни, които са предмет на ОРЗД.

2.4.3 Оценка на въздействието върху защитата на данните

82. Предвид мащаба и чувствителността на личните данни, които могат да бъдат генерирани чрез свързани превозни средства, съществува вероятност обработването — особено в ситуации, при които личните данни се обработват извън превозното средство — често да води до висок риск за правата и свободите на физическите лица. Когато случаят е такъв, от участниците от промишлеността ще се изисква да извършат оценка на въздействието върху защитата на данните, за да се идентифицират и намалят рисковете, както е подробно описано в членове 35 и 36 от ОРЗД. Дори в случаите, когато не се изисква оценка на въздействието върху защитата на данните, най-добра практика е такава оценка да се извърши възможно най-рано в процеса на проектиране. Това ще позволи на участниците от промишлеността да вземат предвид резултатите от този анализ при избора на дизайн преди въвеждането на новите технологии.

2.5 Информация

83. Преди обработването на лични данни субектът на данни бива информиран за самоличността на администратора на лични данни (например- производителя на превозното средство и оборудването или доставчика на услуги), за целта на обработването, за получателите на данните, за срока, за който ще бъдат съхранявани данните, и за правата на физическото лице съгласно ОРЗД⁴⁵.
84. Освен това производителят на превозното средство и на оборудването, доставчикът на услуги или друг администратор на лични данни следва също така да предостави на субекта на данни следната информация, формулирана по ясен, прост и лесно разбираем начин:

- Z координатите за връзка с длъжностното лице по защита на данните;
- Z целите на обработването, за което личните данни са предназначени, както и правното основание;

⁴³ Работна група по член 29 — Становище 05/2014 относно техническите способности за анонимизиране: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_bg.pdf

⁴⁴ Член 4, точка 5 от ОРЗД. Доклад на Агенцията на Европейския съюз за киберсигурност от 3 декември 2019 г.: <https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices>

⁴⁵ Член 5, параграф 1, буква а) и член 13 от ОРЗД. Вж. също Работна група по член 29, Насоки относно прозрачността съгласно Регламент 2016/679 (РД 260 ред.01), одобрени от ЕКЗД.

- Z изричното посочване на законните интереси, преследвани от администратора или от трета страна, когато тези законни интереси представляват правното основание за обработването;
- Z получателите или категориите получатели на личните данни, ако има такива;
- Z срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;
- Z съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни, ограничаване на обработването на лични данни, осигуряване на възможност за възражение срещу обработването или за преносимост на данните, свързани с физическото лице;
- Z съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено, когато обработването се основава на съгласие;
- Z когато е приложимо, факта, че администраторът възнамерява да предаде личните данни на трета държава или на международна организация, и гаранциите, приложени по отношение на трансфера им;
- Z това дали предоставянето на лични данни е задължително или договорно изискване, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последиствия, ако тези данни не бъдат предоставени;
- Z съществуването на автоматизирано вземане на решения, включително профилиране, когато то поражда значителни правни последиствия за субекта на данни и съществена информация относно използваната логика, и значението на решенията, когато и очакваните последиствия от това обработване за физическото лице. Такъв, по-специално, може да бъде случаят при застраховане на физически лица, основано на начина на използване на превозното средство;
- Z правото на жалба до надзорен орган;
- Z информацията относно по-нататъшно обработване;
- Z в случай на съвместно администриране на данни, ясна и пълна информацията относно отговорностите на всеки администратор на лични данни.

85. В някои случаи личните данни не се събират пряко от засегнатото физическо лице. За илюстрация, производител на превозно средство и оборудване може да разчита на търговец за събирането на информацията относно собственика на превозното средство с цел да предложи услуга за спешна пътна помощ. Когато данните не са били събрани пряко, производителят на превозното средство и оборудването, доставчикът на услуги или друг администратор на лични данни трябва да посочи в допълнение към информацията, описана по-горе, съответните категории лични данни, източника на личните данни и ако е приложимо, дали данните са от публично достъпен източник. Информацията трябва да бъде предоставена от администратора в разумен срок след получаването на данните и **не по-късно от първата от изброените по-долу дати**, в съответствие с член 14, параграф 3 от ОРЗД: i) в срок до един месец от получаването на данните, като се отчитат конкретните обстоятелства, при които личните данни се обработват; ii) при осъществяване на първия контакт със субекта на данни; или iii) ако тези данни се предават на трета страна, преди предаването на данните.

86. Може също да се наложи на субектите на данни да се предоставя нова информация, когато за тях се грижи нов администратор на лични данни. Услуга за пътна помощ,

която взаимодейства със свързани превозни средства, може да бъде предоставяна от различни администратори на лични данни в зависимост от това в коя държава или регион се иска помощта. Новите администратори на лични данни следва да предоставят на физическите лица необходимата информация, когато пресичат границите относно предоставените услуги, при които ще се извършва взаимодействие със свързани превозни средства .

87. Информацията, насочена към субектите на данни, може да бъде представена на части⁴⁶, т.е. чрез разделяне на две равнища на информация: от една страна, информация от първо равнище, която е най-важна за субектите на данни, и от друга страна, информация, която вероятно ще представлява интерес на по-късен етап. Основната информация от първо равнище включва, освен самоличността на администратора на лични данни, целта на обработването и описание на правата на субекта на данни, както и всякаква допълнителна информация относно обработването, която има най-голямо въздействие върху лицата, и обработване, което може да ги изненада. ЕКЗД препоръчва при свързаните превозни средства субектът на данни да бъде информиран за всички получатели при предоставянето на информацията от първото равнище. Както е посочено в насоките на Работната група по член 29 относно прозрачността, администраторите следва да представят на субектите на данни онази информация, която е най-съществена за тях. На практика това обикновено са имената на получателите, така че субектите на данни да знаят кой точно разполага с техните лични данни. Ако администраторите не могат да предоставят имената на получателите, информацията следва да бъде възможно най-конкретна, като се посочат видът получател (например- като се уточни неговата дейност), отрасълът, секторът и подсекторът, както и местонахождението на получателите.
88. Субектите на данни може да бъдат информирани чрез кратки и лесно разбираеми клаузи в договора за продажба на превозното средство, в договора за предоставяне на услуги и/или на всякакъв носител в писмена форма, чрез използване на отделни документи (например- чрез книжката за сервизно обслужване или наръчника на превозното средство) или чрез бордовия компютър.
89. В допълнение към необходимата информация, изисквана съгласно членове 13 и 14 от ОРЗД, биха могли да се използват стандартизирани икони, за да се подобри прозрачността чрез потенциално намаляване на необходимостта от предоставяне на огромни обеми писмена информация на субекта на данни. Те следва да бъдат видими в превозните средства така, че да осигуряват ясен преглед на планираното обработване, който да е разбираем и представен в лесно четима форма. ЕКЗД подчертава значението на стандартизирането на тези икони така, че ползвателят да намира едни и същи символи независимо от марката и модела на превозното средство. Когато например се събират определен вид данни, като данни за местонахождение, превозното средство би могло да има ясна бордова сигнализация (като например светлинен индикатор в превозното средство), с която пътниците да бъдат информирани за събирането на данни.

2.6 Права на субекта на данни

90. Производителите на превозни средства и оборудване, доставчиците на услуги и други администратори на лични данни следва да улесняват контрола на субектите на данни върху техните данни през целия период на обработване чрез внедряването на специални инструменти, осигуряващи ефективни начини за упражняване на техните права, по-конкретно, на достъп до, коригиране или изтриване на лични данни или

⁴⁶ Вж. Работна група по член 29, Насоки относно прозрачността съгласно Регламент 2016/679 (РД260вер.01), одобрени от ЕКЗД.

ограничаване на обработването им, в зависимост от правното основание за обработването, правото им на преносимост на данните, както и правото да отправят възражение.

91. За да се улеснят модификациите в настройките, следва да се внедри система за управление на профилите, в която да се съхраняват предпочитанията на известните водачи и да им се помага лесно да променят по всяко време настройките си за неприкосновеност на личния живот. В системата за управление на профилите следва да бъдат централизирани всички настройки за данни за всяко обработване, по-специално, за да се улеснят достъпът до, премахването и преносимостта на лични данни от системите на превозното средство по искане на субекта на данни. Водачите следва да имат възможност да спират временно или постоянно събирането на определени видове данни във всеки един момент, освен ако няма специално правно основание, на което администраторът да може да разчита, за да продължи да събира конкретни данни. В случай на договор, в който е предоставено персонализирано предлагане въз основа на поведението при управление на превозното средство, това може да означава, че ползвателят ще бъде препратен към стандартните условия на този договор. Тези функции следва да бъдат внедрени в превозното средство, въпреки че може да бъдат осигурявани на субектите на данни и чрез допълнителни средства (например- чрез специално приложение). Освен това с цел да се позволи на субектите на данни бързо и лесно да премахват лични данни, които могат да се съхраняват в арматурното табло на автомобила (например история на GPS навигацията, на сърфирането в интернет и др.), ЕКЗД препоръчва на производителите да предоставят опростена функция (като например бутон за заличаване).
92. Продажбата на свързано превозно средство и последвалата смяна на собствеността също трябва да водят до заличаването на всякакви лични данни, които вече не са необходими за предишните посочени цели, и субектът на данни трябва да може да упражни правото си на преносимост.

2.7 Сигурност

93. Производителите на превозни средства и оборудване, доставчиците на услуги и други администратори на лични данни следва да въведат мерки, които гарантират сигурността и поверителността на обработваните данни, и да вземат всички полезни предпазни мерки, за да предотвратят поемането на контрола от неупълномощено лице. По-конкретно участниците в сектора трябва да обмислят въвеждането на следните мерки:
- Z криптиране на съобщителните канали чрез най-съвременен алгоритъм;
 - Z въвеждане на система за управление на криптографски ключове, която е уникална не за всеки модел, а за всяко отделно превозно средство;
 - Z в случаи на отдалечено съхраняване, криптиране на данни посредством най-съвременни алгоритми;
 - Z редовно обновяване на криптографските ключове;
 - Z защита на криптографските ключове от всякакво оповестяване;
 - Z удостоверяване на автентичността на устройствата, приемащи данните;
 - Z гарантиране на целостта на данните (например чрез хеширане);
 - Z подлагане на достъпа до лични данни на надеждни технически способности за установяване на самоличността на ползвателя (парола, електронен сертификат и др.).

94. По отношение, по-специално, на производителите на превозни средства ЕКЗД препоръчва въвеждането на следните мерки за сигурност:

- Z отделяне на жизненоважните функции на превозното средство от онези, които винаги разчитат на далекосъобщителната връзка (т.нар. информационно-развлекателни функции);
- Z внедряване на технически мерки, които позволяват на производителите на превозни средства бързо да коригират слаби места в сигурността по време на целия жизнен цикъл на превозното средство;
- Z по отношение на жизненоважните функции на превозното средство отдаване на приоритет, доколкото е възможно, на използването на сигурни съобщителни средства, които са специално предназначени за сектора на транспорта;
- Z настройване на система за сигнализация в случай на атака върху системите на превозното средство, с възможност за работа в ограничен режим⁴⁷;
- Z съхраняване в хронология на регистъра на всеки достъп до информационната система на превозното средство, например връщане назад за максимален период от шест месеца, за да се даде възможност за разбиране на произхода на всяка потенциална атака, и периодично извършване на преглед на регистрираната информация за разкриване на възможни аномалии.

95. Тези общи препоръки следва да бъдат допълнени със специфични изисквания, като се вземат предвид характеристиките и целта на всяко обработване на данни.

2.8 Предаване на лични данни на трети страни

96. По принцип само администраторът на лични данни и физическото лице имат достъп до данните, генерирани от свързано превозно средство. Администраторът на лични данни обаче може да предава лични данни на търговски партньор (получател), доколкото такова предаване на данни законосъобразно почива на едно от правните основания, посочени в член 6 от ОРЗД.

97. С оглед на евентуалната чувствителност на данните за използването на превозното средство (например- пропътувани маршрути, стил на управление на превозното средство) ЕКЗД препоръчва системно да се получава съгласието на субекта на данни, преди данните му да бъдат предадени на търговския партньор, който действа като администратор на данни (например чрез поставяне на отметка в поле, което не е предварително означено, или когато това е технически възможно, чрез използване на физическо или логическо устройство, до което лицето може да осъществява достъп от превозното средство). Търговският партньор на свой ред става отговорен за данните, които получава, и подлежи на всички разпоредби на ОРЗД.

98. Производителят на превозни средства, доставчикът на услуги или друг администратор на лични данни може да предава личните данни на обработващ лични данни, който е избран да играе роля в предоставянето на услугата на субекта на данни, при условие че обработващият няма да ги използва за собствени цели. Администраторите и обработващите лични данни съставят договор или друг правен документ, в който се уточняват задълженията на всяка страна и се излагат разпоредбите на член 28 от ОРЗД.

⁴⁷ Ограниченият режим представлява работен режим на превозното средство, с който се гарантира, че жизненоважните функции за безопасната експлоатация на превозното средство (т.е. минималните изисквания за безопасност) ще бъдат гарантирани дори, когато други не толкова важни функции са изключени (например може да се счита, че работата на устройството за географско насочване не е жизненоважна, за разлика от тази на спирачната система).

2.9 Предаване на лични данни извън ЕС/ЕИП

99. Когато се предават лични данни извън Европейското икономическо пространство, се предвиждат специални предпазни мерки, за да се гарантира, че личните данни не губят предвидената защитата.
100. Вследствие на това администраторът на лични данни може да предава лични данни на получател само доколкото такова предаване е в съответствие с изискванията, установени в глава V от ОРЗД.

2.10 Използване на бордови технологии за безжична локална мрежа

101. Напредъкът при клетъчните технологии направи възможно лесното използване на интернет по време на пътуване. Макар че е възможно да се получи WLAN свързаност в превозното средство чрез зона за безжична локална мрежа в смартфон или специално устройство (донгъл за бордова диагностична система (БДС-II), безжичен модем или рутер и др.), в днешно време повечето производители предлагат модели, които включват вградена клетъчна връзка за данни и също така са в състояние да създават безжични локални мрежи. В зависимост от случая следва да се разгледат различни случаи:

ZWLAN свързаност се предлага като услуга от професионален доставчик на услуги за превоз, като таксиметров водач, за неговите клиенти. В този случай професионалният доставчик или неговото дружество може да се счита за доставчик на интернет услуги и съответно подлежи на конкретни задължения и ограничения по отношение на обработването на личните данни на своите клиенти;

ZWLAN свързаността е внедрена само за ползване от водача (само от водача и неговите пътници). В този случай се счита, че обработването на лични данни представлява чисто лични или домашни занимания в съответствие с член 2, параграф 2, буква в) и съображение 18 от ОРЗД.

102. Като цяло широкото разпространение на интерфейси за интернет свързаност чрез WLAN крие повишени рискове за неприкосновеността на личния живот на физическите лица. На практика чрез своите превозни средства ползвателите непрекъснато разпръскват данни и следователно могат да бъдат идентифицирани и проследявани. Поради това, за да се предотврати проследяване, производителите на превозни средства и оборудване следва да поставят лесни за използване възможности за неучастие, които гарантират, че от бордовата локална безжична мрежа не се събира идентификаторът на въпросната WLAN (service set identifier — SSID).

3 ПРАКТИЧЕСКИ КАЗУСИ

103. В този раздел са разгледани пет конкретни примера за обработване при свързаните превозни средства, съответстващи на сценарии, които заинтересованите страни в сектора вероятно ще срещнат. Примерите обхващат обработването на данни, което изисква изчислителна мощност, която не може да бъде мобилизирана на място в превозното средство, и/или изпращането на лични данни на трета страна, която да извърши допълнителен анализ или да предостави допълнителна функционалност от разстояние. За всеки вид обработване в настоящия документ са посочени преследваните цели, категориите на събраните данни, срокът за запазване на тези данни, правата на субектите на данни, мерките за сигурност, които трябва да бъдат приложени, и получателите на информацията. В случай че някои от тези области не са описани по-долу, се прилагат общите препоръки, описани в предишната част.
104. Избраните примери не са изчерпателни и са предназначени да дадат ориентир за различните видове обработване, правни основания, участници и др., които може да бъдат ангажирани в контекста на свързаните превозни средства.

3.1 Предоставяне на услуга от трета страна

105. Субектите на данни може да сключат договор с доставчик на услуги, за да получат услуги с добавена стойност, свързани с тяхното превозно средство. Например, субектът на данни може да сключи договор за застраховане, основано на начина на използване на превозното средство, предлагащ намалени застрахователни премии за по-малко ползване („плащане според ползването на превозното средство“) или за добро

поведение при управление („плащане според поведението при управление на превозното средство), което налага наблюдение от страна на застрахователното дружество на навигациите при управление. Субектът на данни може също така да сключи договор с дружество, което предлага пътна помощ в случай на повреда и което налага предаване на местонахождението на превозното средство на дружеството, или договор с доставчик на услуги, за да получава съобщения или предупреждения, свързани с функционирането на превозното средство (например- предупреждение за състоянието на износване на спирачките или напомняне за датата на техническия преглед).

3.1.1 Застраховане, основано на използването

106. „Плащане според ползването на превозното средство“ е вид застраховане, основано на използването, което проследява пробег и/или навигациите при управление на превозното средство, за да се разграничат и възнаградят „съвестните“ водачи, като им се осигурят по-ниски премии. Застрахователят ще изисква от водача да инсталира вградена телематична услуга — мобилно приложение, или да активира вграден при производството модул, който да проследява изминатите мили и/или поведението при управление на превозното средство (модел на спиране, бързо ускоряване и др.) на титулара на полицата. Информацията, събрана чрез телематичното устройство, ще се използва за определяне на показателите за водача, за да се анализират рисковете, които той може да представлява за застрахователното дружество.
107. Тъй като за застраховането, основано на начина на използването, е необходимо съгласие в съответствие с член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, ЕКЗД посочва, че титлярът на полицата трябва да има избор да подпише застрахователна полица, която не е основавана на този принцип. В противен случай съгласието не би се считало за свободно изразено, тъй като изпълнението на договора би било поставено в зависимост от съгласието. Освен това в член 7, параграф 3 от ОРЗД е предвидено изискване субектът на данни да има правото да оттегли съгласието си.

3.1.1.1 Правно основание

108. Когато данните се събират чрез публично достъпна електронна съобщителна услуга (например чрез SIM картата, съдържаща се в телематичното устройство), ще е необходимо съгласие, за да се получи достъп до информация, която вече се съхранява в превозното средство, както е предвидено в член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Всъщност нито едно от освобождаванията, предвидени в тези разпоредби, не може да се приложи в тази връзка: обработването не се извършва единствено с цел предаване на съобщения по електронна съобщителна мрежа, нито се отнася до услуга на информационното общество, изрично поискана от абоната или ползвателя. Съгласието може да бъде получено по време на сключването на договора.
109. Що се отнася до обработването на лични данни след съхранението или получаването на достъп до крайното оборудване на крайния потребител, застрахователното дружество може да се позове на член 6, параграф 1, буква б) от ОРЗД, при условие че може да установи както това, че обработването се извършва въз основа на валиден договор със субекта на данни, така и че обработването е необходимо, за да може конкретният договор с физическото лице да бъде изпълнен. Доколкото обработването е обективно необходимо за изпълнението на договора със субекта на данни, ЕКЗД счита, че в този конкретен случай позоваването на член 6, параграф 1, буква б) от ОРЗД няма да доведе до намаляване на допълнителната защита, предвидена в член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и

електронни комуникации. Това правно основание се привежда в действие чрез подписването от субекта на данни на договор със застрахователното дружество.

3.1.1.2 Събирани данни

110. Има два вида лични данни, които трябва да бъдат взети предвид:

- Z **търговски данни и данни относно сделки:** информация за идентифициране на субекта на данни, данни, свързани със сделки или с платежни средства, и т.н.;
- Z **данни относно използването:** лични данни, генерирани от превозното средство, навигация при управление на превозното средство, местонахождение и т.н.

111. ЕКЗД препоръчва, доколкото е възможно, и като се има предвид, че с данните, събрани чрез телематичната кутия, може да се злоупотреби за създаването на точен профил на движенията на водача, необработените данни относно поведението при управление на превозното средство да бъдат обработвани:

- Z в рамките на превозното средство в телематични кутии или в смартфона на ползвателя така, че застрахователят да има достъп само до данните за резултатите (например показатели, свързани с навигацията при управление на превозното средство), а не до подробни необработени данни (вж. раздел 2.1);
- Z от доставчика на телематични услуги от името на администратора (застрахователното дружество), за да се генерират цифрови показатели, които се предават на застрахователното дружество на определен период. В този случай необработените данни и данните, пряко свързани със самоличността на водача, трябва да бъдат разделени. Това означава, че доставчикът на телематични услуги получава данните в реално време, но не знае имената, табелите с регистрационните номера и т.н. на титулярите на полици. От друга страна, застрахователят знае имената на титулярите на полици, но получава само показателите и общите километри, а не необработените данни, използвани за извеждане на тези показатели.

112. Освен това трябва да се отбележи, че ако за изпълнението на договора е необходим само пробегът, данните за местонахождение не се събират.

3.1.1.3 Срок за запазване

113. При обработването на данни, което се извършва за изпълнението на договор (т.е. предоставяне на услуга), е важно да се направи разграничение между два вида данни, преди да се определят съответните срокове за запазването им:

- Z **търговски данни и данни относно сделки:** тези данни могат да се пазят в активна база данни за целия срок на договора. В края на договора те могат да бъдат архивирани физически (на отделен носител: DVD и др.) или логически (чрез управление на предоставянето на разрешения) в случай на евентуален съдебен процес. След това в края на законоустановените давностни срокове данните се заличават или анонимизират;
- Z **данни относно използването:** данните относно използването могат да бъдат класифицирани като необработени данни и обобщени данни. Както беше посочено по-горе, ако е възможно, администраторите или обработващите лични данни не следва да обработват необработени данни. Ако е необходимо, необработените данни следва да се съхраняват само докато са необходими за изготвяне на обобщените данни и за проверка на валидността на този процес на агрегиране. Обобщените данни следва да се съхраняват, докато са необходими за предоставянето на услугата, или съгласно изискванията на правото на Съюза или на държава членка.

3.1.1.4 Предоставяне на информация и права на субектите на данни

114. Преди обработването на лични данни субектът на данни бива информиран по прозрачен и разбираем начин съгласно член 13 от ОРЗД. По-специално, той трябва да бъде информиран за срока, за който ще се съхраняват личните данни, или ако това не е възможно, за критериите, използвани за определяне на този срок. В този последен случай, ЕКЗД препоръчва да се възприеме педагогически подход, за да се изтъкне разликата между необработените данни и показателите, получени на тази основа, като се подчертае, когато случаят е такъв, че застрахователят ще събира резултата от показателите само когато е подходящо.
115. Когато данните не се обработват в рамките на превозното средство, а от доставчик на телематични услуги от името на администратора (застрахователното дружество), може да е полезно, ако в информацията се спомене, че в този случай доставчикът няма да има достъп до данни, пряко свързани със самоличността на водача (например имена, табели с регистрационни номера и т.н.). Освен това, като се имат предвид значението на информирането на субектите на данни относно последиците от обработването на личните им данни и фактът, че лицата не следва да бъдат изненадани от обработването на личните си данни, ЕКЗД препоръчва физическото лице да бъде информирано за наличието на профилиране и последиците от такова профилиране дори ако то не включва автоматизирано вземане на решения, както е посочено в член 22 от ОРЗД.
116. По отношение на правото на субектите на данни, те биват изрично информирани за наличните средства за упражняване на правото си на достъп, коригиране, ограничаване и изтриване. Тъй като необработените данни, събирани за тази цел, се предоставят от субекта на данни (чрез специални формуляри или чрез неговата дейност) и се обработват въз основа на член 6, параграф 1, буква б) от ОРЗД (изпълнение на договор), лицето има право да упражни правото си на преносимост на данните. Както се подчертава в насоките относно правото на преносимост на данните, ЕКЗД настоятелно препоръчва „администраторите на данни ясно да обясняват разликата между видовете данни, които субектът на данните може да получава въз основа на правата на субекта на достъп до данни и преносимост на данните“⁴⁸.
117. Информацията може да бъде предоставена при подписване на договора.

3.1.1.5 Получател:

118. ЕКЗД препоръчва, доколкото е възможно, данните относно използването на превозно средство да се обработват директно в телематични кутии така, че застрахователят да има достъп само до данните за резултатите (например показателите), а не до подробни необработени данни.
119. Ако доставчикът на телематични услуги събира данните от името на администратора (застрахователното дружество), за да генерира цифрови показатели, не е необходимо да знае самоличността на водача (като имена, табели с регистрационни номера и т.н.) или на титулярите на полиците.

3.1.1.6 Сигурност:

120. Прилагат се общите препоръки. Вж. раздел 2.7.

3.1.2 Наемане и резервиране на място за паркиране

121. Собственикът на място за паркиране може да поиска да го отдаде под наем. За тази цел той обявява мястото в уеб приложение и определя цена за него. Впоследствие, след като мястото за паркиране бъде обявено, собственикът бива уведомяван чрез

⁴⁸ Работна група по член 29, Насоки относно правото на преносимост на данните съгласно Регламент 2016/676, РД 242 ред.01, одобрени от ЕКЗД, стр. 13.

приложението, когато водач иска да го резервира. Водачът може да избере местоназначение и да провери за налични места за паркиране въз основа на множество критерии. След одобрението на собственика сделката се потвърждава и доставчикът на услуги обработва платежната операция, след което водачът използва навигация, за да стигне до местонахождението.

3.1.2.1 Правно основание

122. Когато данните се събират чрез публично достъпна електронна съобщителна мрежа, се прилага член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.
123. Тъй като това е услуга на информационното общество, съгласно член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации не се изисква съгласие за получаване на достъп до информация, която вече се съхранява в превозното средство, когато такава услуга е изрично поискана от абоната.
124. За обработването на лични данни и само за данни, необходими за изпълнението на договора, по който субектът на данни е страна, правното основание ще бъде член 6, параграф 1, буква б) от ОРЗД.

3.1.2.2 Събирани данни

125. Обработваните данни включват координатите за връзка с водача (име, електронна поща, телефонен номер, тип превозно средство (например- автомобил, камион, мотоциклет), табелата с регистрационен номер, периода на престой на паркинг, данните относно плащането (например- информация за кредитна карта), както и навигационни данни.

3.1.2.3 Срок за запазване

126. Данните следва да се пазят само докато са необходими за изпълнението на договора за паркиране или съгласно изискванията, предвидени в правото на Съюза или на държава членка. След това данните се анонимизират или заличават.

3.1.2.4 Предоставяне на информация и права на субектите на данни

127. Преди обработването на лични данни субектът на данни следва да бъде информиран по прозрачен и разбираем начин съгласно член 13 от ОРЗД.
128. Субектът на данни следва да бъде изрично информиран за наличните средства за упражняване на правото си на достъп, коригиране, ограничаване и изтриване. Тъй като данните, събирани за тази цел, се предоставят от субекта на данни (чрез специални формуляри или чрез неговата дейност) и се обработват въз основа на член 6, параграф 1, буква б) от ОРЗД (изпълнение на договор), лицето има право да упражни правото си на преносимост на данните. Както се подчертава в насоките относно правото на преносимост на данните, ЕКЗД настоятелно препоръчва „администраторите на данни ясно да обясняват разликата между видовете данни, които субектът на данните може да получава въз основа на правата на субекта на достъп до данни и преносимост на данните“.

3.1.2.5 Получател

129. По принцип достъп до данните имат само администраторът и обработващият лични данни.

3.1.2.6 Сигурност:

130. Прилагат се общите препоръки. Вж. раздел 2.7.

3.2 Система за автоматични спешни повиквания

131. В случай на тежко произшествие в Европейския съюз превозното средство автоматично задейства системата за автоматични спешни повиквания до 112 — общоевропейския номер за спешни повиквания (вж. раздел 1.1 за допълнителни подробности), което позволява незабавното изпращане на линейка до мястото на произшествието съгласно Регламент (ЕС) 2015/758 от 29 април 2015 г. относно изискванията за одобряване на типа по отношение на въвеждането на бордовата система eCall, основаваща се на услугата 112, и за изменение на Директива 2007/46/ЕО (наричан по-нататък „Регламент (ЕС) 2015/758“).
132. Всъщност генераторът на системата, монтиран в превозното средство, който позволява предаване чрез обществена мобилна безжична съобщителна мрежа, инициира спешно повикване, което се задейства автоматично от датчиците на превозното средство или ръчно от пътуващите в превозното средство само в случай на произшествие. В допълнение към активирането на звуковия канал второто събитие, задействано автоматично в резултат на произшествие, се състои от генериране на минималния набор от данни (МНД) и изпращането му до обществения център за приемане на спешни повиквания (ОЦСП).

3.2.1 Правно основание

133. Във връзка с прилагането на Директивата за правото на неприкосновеност на личния живот и електронни комуникации трябва да се вземат предвид две разпоредби:
- Z член 9 относно данни за местонахождение, различни от данни за трафика, които се прилагат само за електронни съобщителни услуги;
 - Z член 5, параграф 3 за получаване на достъп до информация, съхранявана в генератора, монтиран в превозното средство.
134. Въпреки факта, че по принцип тези разпоредби изискват съгласието на субекта на данни, с Регламент (ЕС) 2015/758 се установява правно задължение, на което администраторът на лични данни подлежи (субектът на данни няма истински или свободен избор и няма да може да откаже обработването на своите данни). Следователно с Регламент (ЕС) 2015/758 се отменя необходимостта от съгласието на водача за обработването на данни за местонахождение и МНД⁴⁹.
135. Правното основание за обработването на тези данни ще бъде спазването на законово задължение, както е предвидено в член 6, параграф 1, буква в) от ОРЗД (т.е. Регламент (ЕС) 2015/758).

3.2.2 Събирани данни

136. Регламент (ЕС) 2015/578 предвижда, че данните, изпращани от бордовата система за автоматични спешни повиквания, основаваща се на телефон 112, съдържат единствено минималната информация, посочена в стандарта EN 15722:2015 „Интелигентни транспортни системи. Електронна сигурност. Минимален набор от данни (МНД) за система за електронно повикване“, включително:
- Z посочване дали системата е задействана ръчно или автоматично;

⁴⁹ Трябва да се отбележи, че в член 8, параграф 1, буква е) от мандата на Съвета за водене на преговори относно предложението за Регламент за неприкосновеността на личния живот и електронните съобщения е предвидено конкретно изключение за системата, тъй като не е необходимо съгласие, когато „*трябва да се определи местоположението на крайно оборудване, когато краен ползвател отпрати спешно повикване до единния европейски номер за спешни повиквания 112 или до национален номер за спешни повиквания, в съответствие с член 13, параграф 3*“.

- Z типа превозно средство;
- Z идентификационния номер на превозното средство (ИНПС);
- Z типа задвижване на превозното средство;
- Z електронния времеви печат на първоначалното генериране на съобщение с данни в рамките на текущото събитие на произшествието, при което се задейства системата;
- Z последната известна географска ширина и географска дължина на местонахождението на превозното средство, определени във възможно най-късния момент преди генерирането на съобщението;
- Z последната известна истинска посока на движение, определена във възможно най-късния момент преди генерирането на съобщението (само последните три местонахождения на превозното средство).

3.2.3 Срок за запазване

137. Регламент (ЕС) 2015/758 предвижда, че данните не се пазят по-дълго от необходимото за справяне с извънредни ситуации. Тези данни се заличават изцяло, след като престанат да са необходими за тази цел. Освен това във вътрешната памет на системата за автоматични спешни повиквания, основаваща се на телефон 112, данните автоматично и непрекъснато се заличават. Позволява се съхранението само на последните три местонахождения на превозното средство, доколкото това е строго необходимо за определянето на местонахождението и посоката на движение в момента на събитието.

3.2.4 Предоставяне на информация и права на субектите на данни

138. Член 6 от Регламент (ЕС) 2015/758 предвижда производителите да предоставят ясна и пълна информация за обработването на данни, извършвано посредством системата за автоматизирани спешни повиквания. Тази информация се предоставя в ръководството за употреба поотделно за бордовата система, основаваща се на телефон 112, и за системата, поддържана от услуги на трети страни. Тя включва:

- Z препратка към правното основание за обработването;
- Z факта, че бордовата системата за автоматични спешни повиквания, основаваща се на телефон 112, е активирана по подразбиране;
- Z реда и условията на обработването на данни, което се извършва от бордовата система за автоматични спешни повиквания, основаваща се на телефон 112;
- Z конкретните цели на обработването на данни в системата, което следва да е ограничено до извънредните ситуации, посочени в член 5, параграф 2, първа алинея от Регламент (ЕС) 2015/758;
- Z видовете данни, които се събират и обработват, и получателите на тези данни,
- Z срока за запазване на данните в бордовата система, основаваща се на телефон 112;
- Z факта, че няма постоянно проследяване на превозното средство;
- Z реда и условията за упражняването на правата на субектите на данни, както и службата за контакт, компетентна да обработва искания за достъп;
- Z всяка необходима допълнителна информация относно проследимостта, проследяването и обработването на лични данни във връзка с използването на системата, поддържано от услуги на трети страни (TPS eCall), и/или други услуги с добавена стойност, за което се изисква изрично съгласие от страна на ползвателя и е в съответствие с ОРЗД. Отчита се

по-специално фактът, че може да има разлики между обработването на данни, извършено чрез бордовата система, основаваща се на телефон 112, и бордовите системи TPS eCall или чрез други услуги с добавена стойност.

139. Освен това доставчикът на услуги трябва да предостави на субектите на данни информация по прозрачен и разбираем начин в съответствие с член 13 от ОРЗД. По-специално, те трябва да бъдат информирани за целите на обработването, за които са предназначени личните данни, както и за факта, че обработването на лични данни се основава на правно задължение, на което администраторът е обект.
140. В допълнение, като се вземе предвид естеството на обработването, информацията за получателите или категориите получатели на личните данни следва да бъде ясна и субектите на данни следва да бъдат информирани, че данните не са достъпни извън бордовата система, основаваща се на телефон 112, за нито един орган преди задействането на системата.
141. По отношение на правата на субектите на данни трябва да се отбележи, че тъй като обработването се основава на законово задължение, правото на възражение и правото на преносимост няма да се прилагат.

3.2.5 Получател

142. Данните не са достъпни извън бордовата система за автоматизирани спешни повиквания, основаваща се на телефон 112, за нито един орган преди задействането ѝ.
143. Когато се задейства (ръчно от пътуващите в превозното средство или автоматично, веднага щом монтиран в превозното средство датчик засече тежък сблъсък), системата установява гласова връзка със съответния ОЦСП и МНД се изпраща на оператора на ОЦСП.
144. Освен това данните, предавани чрез бордовата система, основаваща се на телефон 112, и обработвани от ОЦСП, могат да бъдат предавани на службите за спешно реагиране и службите партньори, посочени в Решение № 585/2014/ЕС, единствено в случай на произшествия, свързани с тази система, и при условията, определени в това решение, и се използват единствено за постигане на целите на същото решение. Данните, обработвани от ОЦСП чрез бордовата система, основаваща се на телефон 112, не се предават на трети лица без изричното предварително съгласие на субекта на данни.

3.2.6 Сигурност

145. В Регламент (ЕС) 2015/758 са посочени изискванията за включване в системата за автоматични спешни повиквания на технологии, които укрепват защитата на неприкосновеността на личния живот, за да се предложат на ползвателите подходящото равнище на защита на неприкосновеността на личния живот, както и гаранциите, необходими за предотвратяване на наблюдение и злоупотреби. Освен това производителите следва да гарантират, че бордовата система, основаваща се на телефон 112, и всяка друга инсталирана система за спешно повикване, която се поддържа от услуги на трети страни, или услуга с добавена стойност са проектирани по такъв начин, че между тях не е възможен обмен на лични данни.
146. По отношение на ОЦСП държавите членки следва да гарантират, че личните данни са защитени от злоупотреби, включително незаконен достъп, промяна или загуба, и че на съответното равнище са установени и се спазват надлежно протоколи относно съхраняването на личните данни, продължителността на запазването, обработването и защитата им.

3.3 Проучвания на произшествия

147. Субектите на данни могат доброволно да се съгласят да участват в проучвания на произшествия, насочени към по-добро разбиране на причините за пътнотранспортните произшествия и за по-общи научни цели.

3.3.1 Правно основание

148. Когато данните се събират чрез публично достъпна електронна съобщителна услуга, администраторът на лични данни ще трябва да събере съгласието на субекта на данни за получаване на достъп до информация, която вече се съхранява в превозното средство, както е предвидено в член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Всъщност нито едно от освобождаванията, предвидени в тези разпоредби, не може да се приложи в този случай: обработването не се извършва единствено с цел предаване на съобщения по електронна съобщителна мрежа, нито се отнася до услуга на информационното общество, изрично поискана от абоната или ползвателя.
149. По отношение на обработването на лични данни и като се вземат предвид разнообразието и количеството лични данни, необходими за проучвания на произшествия, ЕКЗД препоръчва обработването да се основава на предварителното съгласие на субекта на данни съгласно член 6 от ОРЗД. Такова предварително съгласие трябва да бъде предоставено на специален формуляр, чрез който субектът на данни доброволно се съгласява да участва в проучването и личните му данни да бъдат обработвани за тази цел. Съгласието е свободното, конкретно и информирано волеизявление на лицето, чиито данни се обработват (например чрез поставяне на отметка в поле, което не е отменено предварително, или конфигуриране на бордовия компютър, за да се активира дадена функция в превозното средство). Това съгласие трябва да се предоставя отделно, за конкретни цели; то не може да бъде включвано в договора за закупуване или наемане на нов автомобил и трябва да може да се оттегля толкова лесно, колкото е дадено. Оттеглянето на съгласието води до спиране на обработването. След това данните следва да бъдат заличени от активната база данни или анонимизирани.
150. Съгласието, което се изисква по член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, и съгласието, необходимо като правно основание за обработването на данни, могат да бъдат получени едновременно (например чрез поставяне на отметка в поле, където ясно се посочва с какво се съгласява субектът на данни).
151. Трябва да се отбележи, че в зависимост от условията на обработването (характера на администратора на лични данни и т.н.) законно може да бъде избрано друго правно основание, при условие че не се намалява допълнителната защита, предвидена в член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации (вж. точка 15). Ако обработването се основава на друго правно основание, като например изпълнението на задача от обществен интерес (член 6, параграф 1, буква д) от ОРЗД), ЕКЗД препоръчва субектите на данни да бъдат включени в проучването на доброволна основа.

3.3.2 Събирани данни

152. Администраторът на данни събира само лични данни, които са строго необходими за обработването.
153. Има два вида данни, които трябва да се вземат предвид:

Z данни, отнасящи се до участниците и превозните средства;

Z технически данни от превозните средства (моментна скорост и др.).

154. Научните изследвания, свързани с произшествията, дават основание за събирането на данни за моментната скорост, включително от юридически лица, които не предоставят обществена услуга в тесния смисъл.
155. Всъщност, както беше отбелязано по-горе, ЕКЗД счита, че данните за моментната скорост, събирани във връзка с проучване на произшествие, не са свързана с престъпление информация по местоназначение (т.е. те не се събират с цел разследване или наказателно преследване на престъпление), което оправдава събирането им от юридически лица, които не предоставят обществена услуга в тесния смисъл.

3.3.3 Срок за запазване

156. Важно е да се прави разлика между два вида данни. Първо, данните, свързани с участниците и превозните средства, могат да бъдат пазени за периода на проучването. Второ, техническите данни от превозните средства следва да се пазят възможно най-кратко за целта. В това отношение пет години от крайната дата на проучването изглежда са разумен срок. В края на този срок данните се заличават или анонимизират.

3.3.4 Предоставяне на информация и права на субектите на данни

157. Преди обработването на лични данни субектът на данни бива информиран по прозрачен и разбираем начин съгласно член 13 от ОРЗД. По-специално, в случай на събиране на данни относно моментната скорост субектите на данни следва да бъдат изрично информирани за събирането на данни. Тъй като обработването на данни се основава на съгласие, физическото лице следва да бъде изрично информиран за съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено. Освен това, тъй като събраните данни се предоставят от субекта на данни (чрез специфични форми или чрез неговата дейност) и се обработват въз основа на член 6, параграф 1, буква а) от ОРЗД (съгласие), лицето има право да упражни правото си на преносимост на данните. Както се подчертава в насоките относно правото на преносимост на данните, ЕКЗД настоятелно препоръчва „администраторите на данни ясно да обясняват разликата между видовете данни, които субектът на данните може да получава въз основа на правата на субекта на достъп до данни и преносимост на данните“. Следователно, администраторът на лични данни следва да осигури лесен начин за свободно оттегляне на съгласието му по всяко време, както и да разработи инструменти, за да може да отговаря на искания за преносимост на данните.
158. Тази информация може да бъде предоставена при подписване на формуляра за даване на съгласие за участие в проучването на произшествия.

3.3.5 Получател

159. По принцип достъп до данните имат само администраторът и обработващият лични данни.

3.3.6 Сигурност

160. Както беше отбелязано по-горе, въведените мерки за сигурност се адаптират към степента на чувствителност на данните. Например, ако като част от проучването на произшествието бъдат събрани данни относно моментната скорост (или някакви други данни, свързани с присъди и престъпления), ЕКЗД настоятелно препоръчва да се въведат строги мерки за сигурност, като например:

- Z прилагане на мерки за псевдонимизация (например хеширане с помощта на секретен ключ на данни, като фамилното име/собственото име на субекта на данни и серийния номер);
- Z съхраняване на данни, свързани с моментната скорост и местонахождението, в отделни бази данни (например с помощта на най-съвременен механизъм за криптиране с отделни ключове и механизми за одобрение);
- Z и/или заличаване на данни за местонахождение веднага щом съответното събитие или последователност бъдат квалифицирани (например вид на пътя, ден/нощ) и съхранение на данни за директно идентифициране в отделна база данни, до която имат достъп само малък брой хора.

3.4 Борба с кражбите на автомобили

161. В случай на кражба субектите на данни може да пожелаят да се опитат да намерят своето превозно средство, като използват данни относно неговото местонахождение. Използването на данни за местонахождение е ограничено до конкретните нужди на разследването и до оценката на случая от страна на компетентните съдебни органи.

3.4.1 Правно основание

162. Когато данните се събират чрез публично достъпна електронна съобщителна услуга, се прилага член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.
163. Тъй като това е услуга на информационното общество, съгласно член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации не се изисква съгласие за получаване на достъп до информация, която вече се съхранява в превозното средство, когато такава услуга е изрично поискана от абоната.
164. По отношение на обработването на лични данни правното основание за обработване на данните за местонахождение ще бъде съгласието на собственика на превозното средство или, ако е приложимо, изпълнението на договор (само за данни, необходими за изпълнението на договора, по който собственикът на превозното средство е страна).
165. Съгласието е свободното, конкретно и информирано волеизявление на лицето, чиито данни се обработват (например чрез поставяне на отметка в поле, което не е отметнато предварително, или конфигуриране на бордовия компютър, за да се активира дадена функция в превозното средство). Свободата на даване на съгласие включва възможността за оттегляне на съгласието по всяко време, за което субектът на данни следва да бъде изрично информиран. Оттеглянето на съгласието води до спиране на обработването. След това данните следва да бъдат заличени от активната база данни, анонимизирани или архивирани.

3.4.2 Събирани данни

166. Данни за местонахождение могат да бъдат предавани само след декларирането на кражба и не могат да се събират непрекъснато през останалото време.

3.4.3 Срок за запазване

167. Данните за местонахождение могат да се пазят само за периода, през който случаят се оценява от компетентните съдебни органи, или до края на процедура за разсейване на съмненията, когато тя не завършва с потвърждение на кражбата на превозното средство.

3.4.4 Информирание на субектите на данни

168. Преди обработването на лични данни субектът на данни следва да бъде информиран по прозрачен и разбираем начин съгласно член 13 от ОРЗД. По-конкретно, ЕКЗД препоръчва администраторът на лични данни да подчертае, че няма постоянно проследяване на превозното средство и че данните за местонахождение могат да се събират и предават само след декларирането на кражба. Освен това администраторът трябва да предостави на субекта на данни информация, че до данните имат достъп само одобрени служители на платформата за наблюдение от разстояние и законово одобрени органи.
169. По отношение на правата на субектите на данни, когато обработването на данни се основава на съгласие, субектът на данните следва да бъде изрично информиран за съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено. Освен това, когато данните, събирани за тази цел, се предоставят от него (чрез специални формуляри или чрез неговата дейност) и се обработват въз основа на член 6, параграф 1, буква а) (съгласие) или буква б) (изпълнение на договор) от ОРЗД, субектът на данни има право да упражни правото си на преносимост на данните. Както се подчертава в насоките относно правото на преносимост на данните, ЕКЗД настоятелно препоръчва „администраторите на данни ясно да обясняват разликата между видовете данни, които субектът на данните може да получава въз основа на правата на субекта на достъп до данни и преносимост на данните“.
170. Следователно, администраторът на лични данни трябва да осигури лесен начин за свободно оттегляне на съгласието му по всяко време (само когато съгласието е правното основание), както и да разработи инструменти, за да може да отговоря на искания за преносимост на данните.
171. Информацията може да бъде предоставена при подписване на договора.

3.4.5 Получатели

172. В случай на деклариране на кражба данните за местонахождение могат да бъдат предавани на i) одобрените служители на платформата за наблюдение от разстояние; и ii) на законово одобрените органи.

3.4.6 Сигурност

173. Прилагат се общите препоръки. Вж. раздел 2.7.