Договор за обработка по поръчка (съгласно чл. 28 от Общия регламент относно защитата на данните)

между

Потребителя (както е дефинирано в Основния договор)

(по-долу наречен „**Възложител**“)

и

TB Digital Services GmbH, Oskar-Schlemmer-Str. 19 - 21, 80807 München

(по-долу наречена „**Изпълнител**“)
(Възложителят и Изпълнителят по-долу са наречени поотделно „**Страна**“, а заедно – „**Страните**“).

Увод

(A) Този договор за обработка по поръчка (по-долу „**Договорът**“) се прилага за всички дейности, при които Изпълнителят има достъп до личните данни (както е дефинирано в цифра 1.5 долу) на Възложителя, на трети доставчици или на други засегнати лица във връзка с описаната в цифра 2 дейност от Общите рамкови условия за ползване на платформата и евентуално сключените отделни договори за други услуги (по-долу „**Основен договор**“).

(B) Съгласно този Договор Възложителят е отговорно лице, а Изпълнителят обработва по поръчка в рамките на обработка по поръчка съгласно чл. 28 от Общия регламент относно защитата на данните (както е дефинирано долу).

Страните се договарят следното:

1 Дефиниции и интерпретации

1.1 „**Европейско право**“ е приложимото право на Европейския съюз, приложимите закони на настоящите държави членки на Европейския съюз, както и приложимите закони на всяка отделна държава, която впоследствие е станала членка на Европейския съюз.

1.2 „**Европейско право за защита на личните данни**“ е приложимото право на Европейския съюз за обработка на лични данни (по-специално Общия регламент относно защитата на данните), приложимите закони на настоящите държави членки на Европейския съюз за обработка на личните данни (по-специално Федералния закон за защита на личните данни в съответно валидната му редакция), както и приложимите закони на всяка отделна държава във връзка с обработката на лични данни, която държава впоследствие е станала членка на Европейския съюз.

1.3 „**DS-GVO**“ е РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година 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 (Общ регламент относно защитата на данните)”

1.4 „**BDSG**“ е Федералният закон за защита на личните данни.

1.5 „**Лични данни**“ има същото значение, както е дефинирано във Федералния закон за защита на личните данни/в Общия регламент относно защитата на данните.

2 Предмет на обработката на данните/задължения на Възложителя

2.1 Този Договор регламентира задълженията на Страните във връзка с обработката на личните данни на Възложителя от страна на Изпълнителя в рамките на посочения в Приложение 1 Основен договор.

2.2 Предметът и срокът на обработката, видът и целта на обработката, видът на личните данни, категориите засегнати лица и задълженията и правата на отговорните лица са посочени в Приложение 1 от този Договор и описанието на услугата в Основния договор.

2.3 Възложителят остава отговорен по смисъла на Общия регламент относно защитата на данните и гарантира допустимостта на обработката на личните данни на субектите на данните (шофьори и евентуално други лица). В тази връзка Възложителят по-специално спазва своето всеобхватно задължение да предоставя информация и гарантира, че обработването на лични данни се основава на правна основа за защита на данните (например сключване на дружествено споразумение, ограничаване на обработката за целите на трудовото отношение).

3 Задължения на Изпълнителя

3.1 Изпълнителят обработва личните данни на Възложителя само за посочените в Приложение 1 цели и в рамките на Основния договор, както и по поръчка, и съгласно документираните в Приложение 1 инструкции на Възложителя; Изпълнителят не обработва личните данни съгласно този Договор за никакви други цели. Това не засяга обработката извън този Договор за собствени цели по цифра 8.3.4 от Основния договор. Копия или дубликати от личните данни не могат да се издават без знанието на Възложителя. Това изключва защитени копия, доколкото е необходимо гарантирането на обработката на данни според изискванията, както и данни, които са необходими по отношение на спазването на законните задължения за съхранение.

3.2 След приключване на предоставянето на услугите за обработка Изпълнителят трябва или да върчи всички лични данни на Възложителя по негов избор, и/или да ги изтрие съгласно изискванията за защита на данни, ако това не противоречи на законните срокове за съхранение и доколкото Изпълнителят не ги обработва за собствени цели извън рамките на

този Договор съгласно цифра 8.3.4. от Основния договор. Същото важи за тестови и бракувани материали. Пълното изтриване, респективно предаване, на данните на Възложителя при поискване трябва да се потвърди писмено пред него, като се посочи и датата.

3.3 Ако се включва в обхвата на услугите, Изпълнителят подпомага Възложителя при изпълнението на правата на субекта на данните (справка, коригиране, възражение, изтриване) съгласно инструкциите на Възложителя.

3.4 Изпълнителят потвърждава, че – доколкото е законово необходимо – е назначил упълномощено лице за обработка на личните данни (сравнете § 38 от Федералния закон за защита на личните данни, чл. 37 от Общия регламент относно защитата на данните).

3.5 Изпълнителят се задължава незабавно да информира Възложителя за резултата от проверките на надзорните органи за защита на личните данни, ако те са свързани с обработката на данните на Възложителя. Установените възражения се отстраняват от Изпълнителя в рамките на съобразен срок и Възложителят се информира за тях.

3.6 Обработката на данните от Изпълнителя и одобрен от Възложителя подизпълнител се извършва само на територията на Федерална република Германия, в държава членка на Европейския съюз или в друга държава по договор, съгласно Споразумението за Европейското икономическо пространство. Всяко преместване в друга държава (по-долу „**Трета държава**“) изисква предварителното изрично съгласие на Възложителя и освен това може да последва само тогава, когато са изпълнени специалните изисквания за преместване на данни в Трети държави (сравнете чл. 40 и сл. от Общия регламент относно защитата на данните). За тази цел е евентуално необходимо да се приложат данните в Приложение 1 и допълнителни (договорни) документи.

3.7 При извършването на работата Изпълнителят трябва да информира заетите служители за меродавните за тях предписания за защита на данните и да ги обвърже със задължението за поверителност на данните (сравнете чл. 28 от Общия регламент относно защитата на данните, параграф 3 б), както и да гарантира с подходящи мерки, че всеки служител обработва лични данни само по нареждане на Възложителя.

3.8 Изпълнителят постоянно контролира спазването на предписанията за защита на личните данни по този Договор и документираните инструкции на Възложителя за времето на целия срок на Договора. Резултатите от контрола се представят на Възложителя при поискване, ако те са релевантни за обработката на данните на Възложителя. Мерките за контрол трябва да се опишат в концепция за защита на данните, която се представя на Възложителя при поискване.

3.9 Изпълнителят трябва да подпомогне Възложителя с подходящи технически и организационни мерки с оглед на вида на обработката и според възможността, за да изпълни задължението си за отговор на заявления за упражняване на посочените права на

засегнатите лица в глава III от Общия регламент относно защитата на данните. Възложителят поема възникналите за Изпълнителя разходи в тази връзка.

3.10 Изпълнителят трябва да подпомогне Възложителя с оглед на вида и обработката на предоставената му информация при спазването на посочените задължения в член 32 до 36 от Общия регламент относно защитата на данните.

4 Технически и организационни мерки за сигурност на данните

4.1 Изпълнителят трябва да вземе подходящи технически и организационни мерки за защита на данните (сравнете чл. 32 от Общия регламент относно защитата на данните) Изпълнителят по-специално е задължен да прилага договорените в Приложение 2 към този Договор технически и организационни мерки. Тези мерки се приспособяват от Изпълнителя в хода на поръчката във връзка с техническото и организационното развитие, без това да понижи нивото на защита. Съществените промени се договарят писмено.

4.2 Изпълнителят при запитване доказва на Възложителя фактическото спазване на техническите и организационните мерки.

4.3 Изпълнителят е задължен да води подходяща документация за обработката на данните, чрез която Възложителят да може да удостовери обработката на данни съобразно изискванията. Удостоверяването може да стане чрез одобрена процедура по сертифициране съгласно член 42 от Общия регламент относно защитата на данните.

5 Подизпълнител

5.1 На Изпълнителя е позволено да включи посочените в Приложение 1 подизпълнители.

5.2 Включването на други подизпълнители генерално е позволено. Изпълнителят обаче трябва да информира Възложителя за всяка планирана промяна във връзка с привличането или замяната на подизпълнители; Възложителят може да възрази срещу планираните промени. Като отношение с подизпълнител по смисъла на тази регулация не се разбират такива услуги, които Изпълнителят е възложил при трети лица като допълнителна работа за подпомагане на извършването на поръчката. Към това се числят например телекомуникационни услуги, чистачи, проверяващи или изхвърлянето на носители на данни. Изпълнителят все пак е задължен с цел гарантиране на защитата и сигурността на данните на Възложителя, също и при възложени услуги на трети лица, да сключи подходящи и законни договори, както и да предприеме мерки за контрол.

5.3 Ако Изпълнителят възложи работа на подизпълнител, Изпълнителят трябва да гарантира, че по силата на (i) сключен между подизпълнителя и Изпълнителя договор или (ii) друг правен инструмент съгласно Европейското право за защита на данните същият е обвързан със задължения за защита на данните, каквито са валидни и за Изпълнителя съгласно този Договор. При това Изпълнителят по-специално трябва да гарантира, че подизпълнителят

предлага достатъчно гаранции, че подходящите технически и организационни мерки ще бъдат така проведени, че обработката на личните данни ще съответства на изискванията на Общия регламент относно защитата на данните. При писмено поискване от страна на Възложителя, Изпълнителят трябва да предостави на Възложителя справка за съществото съдържание на договора и прилагането на задълженията, релевантни за защитата на личните данни, ако е необходимо и чрез преглед на релевантните договорни документи. Изпълнителят има право да затъмни търговските условия. Възложителят е длъжен да пази в тайна придобитата информация.

6 Контролни права

6.1 Възложителят има право да контролира сам спазването на задълженията от този Договор (включително предоставените инструкции) или да възложи контрола на посочено от Възложителя подходящо трето лице.

6.2 Изпълнителят гарантира на Възложителя подходяща помощ при контролирането. По-специално Изпълнителят гарантира достъп до съоръженията за обработка на данните и предоставя необходимите справки.

6.3 В случай че контролът доведе до такъв резултат, че Изпълнителят и/или обработката не са спазили предписанията на този Договор и/или европейското право за защита на данните, Изпълнителят предприема всякакви мерки за коригиране, които са необходими, за да гарантира спазването на предписанията на този Договор и/или на европейското право за защита на данните.

6.4 Разходите, възникнали на Възложителя при извършването на контрол, са за негова сметка. Разходите, възникнали на Изпълнителя при извършването на контрол от страна на Възложителя, могат да бъдат изискани от Възложителя, ако Възложителят предприеме или възложи контрол повече от веднъж през календарната година.

6.5 Контрол при Изпълнителя трябва да бъде съобщаван своевременно и не може да нарушава извънредно работата на Изпълнителя.

7 Задължения за информация

Изпълнителят осведомява незабавно Възложителя, ако предоставената от Възложителя инструкция според Изпълнителя нарушава европейското право за защита на личните данни. Оспорваната инструкция не трябва да се спазва, докато не бъде изрично изменена или потвърдена от Възложителя. Изпълнителят няма задължение за материалноправна проверка на инструкциите.

При установяване на грешки или нередности при обработката на данните или при съмнение за нарушение на защитата на данните (заедно по-долу „**Инцидент**“), Изпълнителят незабавно трябва да информира Възложителя по подходящ начин. Изпълнителят трябва да

документира процедурата, включително всички обстоятелства около случая, неговите въздействия и всички мерки за отстраняване, и при поискване от Възложителя незабавно писмено или по електронен път да предаде на Възложителя документираната информация.

8 Отговорност и освобождаване

8.1 Изпълнителят носи отговорност за щети, които са причинени преднамерено и/или поради груба небрежност от страна на Изпълнителя или неговите подизпълнители. За щети, базирани на лека небрежност на Изпълнителя или подизпълнителите му, Изпълнителят носи отговорност само тогава, когато е нарушено кардинално задължение. Кардинални задължения са съществените задължения по Договора, които дават възможност за редовно изпълнение на Договора и на чието изпълнение Възложителят разчита и може да разчита. При лека небрежност по отношение на нарушаването на такива кардинални задължения отговорността на Изпълнителя за типични предвидими щети е ограничена.

8.2 Възложителят освобождава Изпълнителя от всички претенции на трети лица (включително засегнатите лица и/или органите за защита на личните данни), щети и разходи, които се базират на нарушение на Възложителя спрямо предписанията на този Договор и/или на европейското право за защита на данните; това не важи, ако Възложителят не е виновен за нарушението или ако Изпълнителят е допринесъл за нарушението.

9 Срок на договора

Срокът на този Договор съответства на срока на Основния договор. С прекратяването на Основния договор поради каквато и да е причина този Договор автоматично се прекратява. Запазва се правото на прекратяване поради важна причина.

10 Други

10.1 Услугите на Изпълнителя по този Договор се заплащат съгласно регламентираните в Основния договор правила за заплащане.

10.2 Ако личните данни на Възложителя при Изпълнителя са застрашени поради мерки на трети лица (като запор или конфискация), поради несъстоятелност или помирително производство или поради други подобни събития, Изпълнителят незабавно трябва да информира Възложителя.

10.3 Ако отделни предписания от този Договор са или станат невалидни, това не засяга валидността на останалите предписания. В случай на невалидност на дадена клауза Страните договарят заместваща клауза, ориентирана в предметно и икономическо отношение към целта на Договора.

10.4 В случай че Великобритания напусне Европейския съюз, Изпълнителят се задължава веднага да сключи всички споразумения и да предприеме всички действия, необходими за законно допускане на обработката на данни според предмета на Договора във Великобритания към датата на напускане. Ако към датата на напускане няма положително решение за съобразността от страна на Европейската комисия, от днешна гледна точка това са по-специално клаузи за стандартна защита на личните данни съгласно чл. 46, параграф 2 в) за предаване на лични данни на лица, на които е възложена обработката им, чието местоположение е в Трети държави, в които не е гарантирано подходящо ниво на защита.

Ако Изпълнителят не изпълни тези задължения, Възложителят има право с действие от датата на напускане на Великобритания на Европейския съюз да изиска от Изпълнителя съответните услуги да бъдат извършени от свързано предприятие, респективно от част от предприятие, с постоянно седалище в Европейския съюз, без това да създава извънредни или допълнителни разходи за Възложителя.

10.5 Този договор за обработка по поръчка е наличен на 18 езика, при което в случай на отклонения предимство има оригиналната версия на немски език.

10.6 Този Договор подлежи на законодателството на Федерална република Германия с изключение на търговското право на ООН. Изключителен компетентен съд е съдът в Мюнхен.

10.7 Следните приложения са съставна част от Договора:

Приложение 1 – описание на обработката по поръчка
Приложение 2 – технически и организационни мерки

ПРИЛОЖЕНИЕ 1 – описание на обработката по поръчка

1 Основен договор

Основен договор по смисъла на цифра 2.1 от основната част на Договора са „Общите рамкови условия за ползване на платформата.“

Заглавие/Страни: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 München/**Потребител**

2 Предмет и срок на поръчката

Предметът на поръчката е посочен в цифра 1 (*Предмет*) и цифра 8 (*Данни на потребителя и защита на данните*) от Основния договор; срокът на поръчката е посочен в цифра 7 (*Сключване на Договора, срок на Договора и права за прекратяване*) от Основния договор.

3 Обхват, вид и цел на обработката на данни/мерки за обработка на данни

Обхватът, видът и целта на обработката на личните данни са посочени в цифра 8 от Основния договор.

Подробности за предмета на поръчката с оглед на обхвата, вида и целта:

За да могат да се предоставят възложените на Изпълнителя услуги (както е дефинирано в Основния договор), Изпълнителят трябва да събере личните данни на Възложителя за свързани превозни средства или мобилни устройства (и евентуално прехвърлени лични данни от трети доставчик, с който потребителят е договорил трети услуги) в необходимия за предоставяне на услугите размер и да ги прехвърли и запамети на платформа на Изпълнителя. Изпълнителят ще обработва запаметените на платформата данни в необходимия размер за целите на предоставяне на услугата (за да може с помощта на личните данни да анализира и оцени поведението при движение на шофьорите, както и ползването на свързаното превозно средство или мобилно устройство, и да предостави на Възложителя базирани на това специално изготвени за него оферти, като обучения за шофьори, детайли по оборудването, както и предложения за повишение на ефективността). Точният обхват, вид и цел са посочени по-специално в допълнително сключените отделни договори.

4 Кръг на засегнатите (категории засегнати лица)

Обработката по поръчка засяга следните кръгове от лица:

- **Шофьори и други служители** (служители на собственото дружество на Възложителя), например
  служители, стажанти, кандидати, бивши служители*;*
- **Шофьори**, които не са служители;

- **Лица за контакт** на товарачите/разтоварачите или други търговски партньори на Възложителя, както и
- **Служители на концерна** (служители на друго дружество от група на Възложителя).

5 Вид на личните данни

Обработката по поръчка обхваща следните видове лични данни:

- Име на шофьора и идентификационен номер на шофьора;
- Идентификационен номер на превозното средство;
- Данни за местоположението;
- Данни за времето за шофиране и почивка;
- Данни за поведението на пътя;
- Данни за състоянието на свързаното превозно средство;
- Данни за състоянието на ремаркето;
- Данни за състоянието на каросериите и полуремаркетата, агрегати и други части на превозното средство;
- Данни за състоянието евентуално на свързани IOT устройства
- Данни за състояние на мобилни устройства;
- Данни за товара;
- Данни за поръчката, както и
- Данни за контакт с лицата за контакт на товарачите/разтоварачите или други търговски партньори на Възложителя.

6 Документирани инструкции

Възложителят инструктира Изпълнителя с настоящото да обработва личните данни така, както е посочено в цифра 8 от Основния договор. Това по-специално включва следната обработка:

- Личните данни се прехвърлят през свързаното превозно средства или мобилно устройство на облачна платформа на Изпълнителя и се записват там.
- Личните данни по този Договор само се обработват, доколкото това е необходимо за изпълнението на Основния договор; цифра 8.3.4 от Основния договор остава незасегната.
- Изпълнителят предава личните данни на трети доставчик (както е дефинирано в Основния договор), ако и доколкото такова предаване на трети доставчик е необходимо, за да предостави той трети услуги (както е дефинирано в Основния договор) на Възложителя.
- С помощта на личните данни Изпълнителят ще анализира и оцени поведението при движение на шофьорите, както и ползването на свързаното превозно средство, и ще предостави на Възложителя базирани на това специално изготвени за него оферти, като обучения за шофьори, детайли по оборудването, както и предложения за повишение на ефективността.

7 Място на обработката

- Германия.
- Обединеното кралство; ако се обработват данни за целите на ИТ хостинг и/или ИТ поддръжка в рамките на Европейския съюз, трябва да се сключат съответните договори за обработка по поръчка.
- Ако за целите на ИТ хостинг и/или ИТ поддръжка Изпълнителят използва подизпълнители извън Европейския съюз (в тази връзка вижте цифра 8 от това Приложение 1), предаването на личните данни става въз основа на сключени между Изпълнителя и подизпълнителя клаузи от стандартния договор/клаузи за стандартна защита на данни за предаване на лични данни на обработващия по поръчка в трети страни съгласно чл. 46, параграф 2 в) от Общия регламент относно защитата на данните.

8 Подизпълнител

Изпълнителят ще използва следните подизпълнители (които евентуално могат да използват други подизпълнители):

№	Подизпълнител (фирма, адрес, лице за контакт)	Категории на обработваните данни	Стъпки на обработка/цел на обработката по поръчка от подизпълнителя
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Всички лични данни на платформата, които имат общо с продажбата (тоест където клиент може да се регистрира на платформата и да прави поръчки)	Хостинг на платформа
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Всички лични данни на платформата, които имат общо с продажбата (тоест където клиент може да се регистрира на платформата и да прави поръчки)	ИТ поддръжка по отношение на платформата
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 САЩ https://aws.amazon.com/de/compliance/contact/	Всички други лични данни на потребителя, които са предадени на Изпълнителя чрез превозното средство	Хостинг на платформа/ИТ поддръжка по отношение на хостинга на платформата
4	Евентуално в бъдеще вместо номер 3: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 САЩ https://aws.amazon.com/de/compliance/contact/	Всички други лични данни на потребителя, които са предадени на Изпълнителя чрез превозното средство	Хостинг на платформа
5	MAN Service und Support GmbH Dachauer Straße 667	Всички лични данни, които са необходими за обработката на запитванията на клиентите	Поддръжка от 1-во ниво

	80995 München Германия	в рамките на поддръжка от 1-во и 2-ро ниво	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 САЩ	Всички лични данни, които са необходими за обработката при изготвяне на фактури/изпълнение на поръчки	Хостинг на платформа (EU Tenant – Gehosted by Amazon Web Services (EU) – вижте цифра 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München Германия	Всички други лични данни на потребителя, които са предадени на Изпълнителя чрез свързаното превозно средство и/или мобилното устройство	Хостинг на платформа
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Германия	Всички други лични данни на потребителя, които са предадени на Изпълнителя чрез превозни средства TBM1/2	Хостинг на платформа
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Швеция	Всички други лични данни на потребителя, които са предадени на Изпълнителя чрез превозното средство	Хостинг на платформа
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Германия	Всички други лични данни на потребителя, които са предадени на Изпълнителя чрез превозното средство	Хостинг на платформа

ПРИЛОЖЕНИЕ 2 – технически и организационни мерки
Техническите и организационните мерки, които трябва да вземе Изпълнителят, за да гарантира адекватно на риска ниво на защита, са описани в концепцията за защита на данни към платформа RIO и по-специално включват:

1. Псевдонимизация

Ако личните данни се ползват за целите на оценяването, които също се изпълняват с псевдонимизирани данни, се прилагат техники на псевдонимизация. При това за всяко поле от данни първо предварително се дефинира дали трябва да бъде псевдонимизирано, защото това би дало възможност за обратна връзка с дадено лице. Кодовете за псевдонимизация се съхраняват в „сейф за данни“, за който е създадено максималното възможно ограничение на достъпа.

2. Кодиране

Мобилните крайни устройства комуникират криптирано с крайната точка посредством индивидуален за устройството сертификат. Данните се препращат криптирано по-нататък в рамките на платформата RIO („Ubiquitous encryption“ или „encryption everywhere“).

3. Гарантиране на поверителността

Всички служители са и ще бъдат информирани за задължението си за поверителност и са писмено задължени да пазят в тайна данните.

Използваната ИТ инфраструктура се предоставя чрез Amazon Web Services (по-долу AWS) в рамките на облак (IaaS & PaaS). Контролът на достъпа се предоставя от центъра за управление на данни на AWS: центровете за данни на AWS с максимално ниво на сигурност използват мерки за електронен надзор на състоянието на техниката и многостепенни системи за контрол на достъпа. В центровете за данни денонощно има обучен персонал по сигурността и достъпът е строго гарантиран на принципа на минималните права и само за целите на системната администрация.

Достъпът до хардуерните компоненти (клиенти) в TB Digital Services GmbH става съгласно валидните в отделния случай подходящи стандартни мерки. Това са например ограничения в достъпа чрез пропускателни устройства (турникети), инсталации за видеонаблюдение, алармени инсталации и/или охранителна служба, електронно или механично обезопасени врати, сгради, обезопасени срещу взлом, документирани правомощия за достъп (посетители, чужди служители) или декларирани области на сигурност.

Контролирането на достъпа обхваща мерки за сигурност на устройства, мрежова сигурност и сигурност на приложения.

Като мерки за сигурност на устройствата в превозното средство се прилагат различни мерки: Мобилните крайни устройства са трайно вградени в превозното средство и разполагат със Secure Boot, тоест няма възможност за зареждане и стартиране на чужда операционна система.

Мобилните крайни устройства комуникират криптирано с крайната точка посредством индивидуален за устройството сертификат. Данните се препращат криптирано по-нататък в рамките на платформата RIO („Ubiquitous encryption“ или „encryption everywhere“). Крайните устройства се поддържат до актуалното състояние на мерките за сигурност чрез редовно пускане на актуализации на сигурността (управление на пачове).

Като мерки за мрежова сигурност се прилагат и различни стандартни мерки: Имплементират се подходящи (съответстващи на състоянието на техниката) изисквания за паролата (дължина, сложност, срок на паролата и др.). Неднократното въвеждане на погрешна комбинация от потребителско име/парола води до (временно) блокиране на потребителското име. Фирмената мрежа е защитена срещу несигурни отворени мрежи чрез защитна стена. Даден процес е приет, когато гарантира редовното снабдяване на мобилните устройства с актуализации на сигурността (OTA – процес). За разкриване, респективно избягване, на атаки на фирмената мрежа (интранет) се използват подходящи технологии (например системи за засичане на проникване). Служителите постоянно се предупреждават за опасностите и рисковете.

Като мерки за сигурност на приложенията се прилагат няколко стандартни мерки:

Релевантните приложения се защитават чрез подходящи механизми за удостоверяване и оторизация срещу неупълномощен достъп. Имплементират се подходящи (съответстващи на състоянието на техниката) изисквания за паролата (дължина, сложност, срок на паролата и др.). За приложенията с особена нужда от защита се използват силни механизми за удостоверяване (например токени, PKI (инфраструктура с публичен ключ). Неднократното въвеждане на погрешна комбинация от потребителско име/парола води до (временно) блокиране на потребителското име. Използваните данни в релевантната процедура са криптирани на носител на данни, използван мобилно. Успешният достъп и опитите за достъп до приложения се протоколират. Генерираните файлове на протокола се съхраняват за подходящ период (минимум 90 дни) и се тестват (на случаен принцип).

Правомощията на потребителите (за достъп и употреба) се гарантират с различни мерки, при което принципно те се дават на установимо лице. Издаването на разрешителни е отговорност на лицето, което отговаря за платформата, и се проверява редовно. Предоставянето на правомощия за достъп става само след дефиниран и документиран процес. Промените на правомощията за достъп се правят на принципа на четирите очи и се документират в регистрационен файл с вписана версия.

Като мерки за контрол или управление на достъпа се прилагат различни мерки: Правата за достъп се дефинират и документират в рамките на концепция за ролите/правомощията и се дават в съответствие с обусловените от задачата изисквания на съответните роли. За техническите администратори са създадени специфични роли/правомощия (които, ако е технически възможно, не предоставят достъп до лични данни). За специализираната поддръжка са създадени специфични роли/правомощия (които не съдържат права за техническа администрация).

Дефинирането на ролите/правомощията и разпределението на ролите/правомощията, ако е технически и организационно възможно, не става от същите лица и в една подлежаща на ревизиране процедура (по одобрение) и е времево ограничено. Директният достъп до бази данни със заобикаляне на концепцията за ролите/правомощията е възможен само за оторизираните администратори на базата данни. Има регулация за употреба на частни носители на данни, респективно употребата на частни носители на данни е забранена. Съществуват обвързващи регулации относно достъпа до данни при външни поддръжки, дистанционни поддръжки и дистанционна работа. Документите и носителите на данни се унищожават/изхвърлят според предписанията за защита на данните (например шредер, кофа за материали със защитени данни) от надеждна фирма за извозване на отпадъци.

Концепцията за ролите/правомощията се актуализира редовно съобразно променящите се структури на организацията на работата (например нови роли) и разпределените роли/правомощия редовно се проверяват (например от началниците) и евентуално се актуализират, респективно отнемат. Провежда се редовен централен контрол относно предоставените стандартни профили. Промененият достъп (писане, изтриване) се протоколира и генерираните файлове на протокола се съхраняват за подходящ период (минимум 90 дни) и се тестват (на случаен принцип).

Като общи мерки за сигурност на предаването се прилагат различни стандартни мерки:

Лицата, на които е възложено предаването, предварително се информират за предприетите мерки за сигурност. Кръгът от получатели се установява предварително, така че да е възможен съответният контрол (удостоверяване). Целият процес на предаване на данните е установен и документиран и извършването на конкретното предаване на данни се протоколира, респективно документира (например потвърждение за получаване, квитанция). Лицата, на които е възложено предаването, предварително извършват проверка на достоверността, пълнотата и верността.

Преди извършване на конкретния пренос на данни се прави проверка на адреса на получателя (например имейл адрес). Преносът на данни по интернет се извършва криптирано (например криптиране на файлове). Целостта на предадените данни, ако е технически възможно, се гарантира чрез употребата на процедури по подписване (електронен подпис). Електронните потвърждения за приемане се архивират в подходяща форма. Нежеланият пренос на данни в интернет се предотвратява чрез подходящи технологии (например прокси, защитна стена).

Освен това, като мерки за осъществяване на разделението между разузнаване и полиция се прилагат следните стандартни мерки:

Съществуват обвързващи регулации относно гарантирането на целта на обработката на личните данни за спазване на разделението между разузнаване и полиция. Събраните данни за определени цели се записват отделно от събраните данни за други цели. Използваните ИТ системи позволяват отделното запаметяване на данни (чрез възможност за доверени лица или концепции за достъп). Извършва се отделяне на данни в системи за тестване и производствени системи. При псевдонимизирани данни кодът, който дава възможност за повторно

идентифициране, се записва или съхранява отделно. При обработка по поръчка или пренос на функции при Изпълнителя се осъществява отделна обработка на данни на различни Възложители. Наличните концепции за роли/правомощия чрез структурата си дават възможност за логично разделяне на обработените данни.

4. Гарантиране на целостта

Като мерки за осъществяване на протоколиране на въведените данни се прилагат различни стандартни мерки:

Промените в правата за достъп, както и всички дейности на администратора, се протоколират. Писменият достъп (въвеждане, промени, изтривания) и промените в полетата с данни се протоколират (например съдържание на нововъведението или променените записи от данни). Осъществява се протоколиране на преносите (например изтегляне) и протоколиране на влизанията в системата.

Ползваните документи за регистрация се документират и архивират с цел проследимост на въведените данни. Протоколирането се осъществява с дата и час, потребител, вид на дейността, програма на приложение и пореден номер на записа от данни. Настройките на протоколирането се документират.

Гарантира се само достъп за четене на файловете на протоколите. Кръгът на упълномощените за достъп до файловете на протоколите е тясно ограничен (например администратор, лице, на което е възложена защитата на данните, проверяващ). Файловете на протоколите се съхраняват за установен период (напр. 1 година) и после се изтриват съобразно изискванията за защита на данните. Файловете на протоколите редовно се анализират автоматично. Анализите на файловете на протоколите се изготвят в псевдонимизирана форма, ако е възможно.

5. Гарантиране на достъпността

Архитектурата сама по себе си е защитена срещу загуба на данни чрез вътрешни механизми за размножаване в рамките на платформата AWS. Освен това, като мерки за сигурност на обекта се прилагат следните стандартни мерки на AWS:

Провеждат се мерки за противопожарна защита (например огнеупорни врати, детектори за дим противопожарни стени, забрана за пушене). Компютрите са защитени от наводнения (например компютърна зала на 1-вия етаж, сензори за вода). Взети са мерки против вибрации (например компютърната зала не е близо до магистрали, релсови пътища, машинни помещения). Компютрите са защитени от електромагнитни полета (например стоманени плочи във външни стени). Взети са мерки срещу вандализъм и кражба (сравнете контрол на достъпа). Компютрите се намират в климатизирани помещения (температурата и влажността на въздуха се регулират чрез климатик). Компютрите са обезопасени срещу импулсни пренапрежения чрез защита срещу пренапрежение. Взети са мерки за гарантиране на постоянно електроснабдяване без смущения (например UPS устройства, агрегати за аварийно захранване).

Масивите от данни редовно се защитават чрез резервни копия в рамките на платформата AWS. Концепцията за резервни копия е документирана и се проверява и актуализира редовно. Медиите за резервни копия са защитени от неупълномощен достъп. Използваните програми за резервни копия съответстват на актуалните стандарти за качество и редовно се актуализират в това отношение. Изграден е дублиращ център за данни (отдалечен от мястото на обработка) и в случай на катастрофа обработката на данните може да се продължи. Различните мерки за контрол на достъпността се документират в план за управление на аварии на AWS.

Преди поръчката за обработка на данни да бъде възложена, Изпълнителят се проверява внимателно и по установени критерии (технически и организационни мерки). В тази връзка се изисква и проверява подробно представяне на проведените от Изпълнителя технически/организационни мерки за защита на личните данни (отговаряне на каталог с въпроси или концепция за защита на данните). В зависимост от количеството и чувствителността на обработените данни тази проверка евентуално се извършва и на място при Изпълнителя. Подходящите сертификати (например ISO 27001) се вземат предвид при избора на Изпълнител. Установяването на пригодността на Изпълнителя се документира в подходяща и разбираема форма.

За обосноваването на поръчката между Възложителя и Изпълнителя се сключва договор за обработка по поръчка. Той подробно и писмено постановява компетенциите и отговорностите, както и задълженията на двете Страни. В случаи че упълномощен доставчик на услуги е със седалище извън ЕС, респективно ЕИП, се прилагат клаузите на ЕС за стандартен договор. В договора се постановява, че обработката на данни от страна на Изпълнителя може да се извършва само в рамките на инструкциите на Възложителя. Изпълнителят се задължава да осведомява незабавно Възложителя, ако една от неговите инструкции според Изпълнителя нарушава предписанията за защита на личните данни. За да се защитят правата на засегнатите лица, в договора за обработка по поръчка се договаря, че Изпълнителят ще окаже подходяща помощ на Възложителя, ако това е необходимо, например в случай на издаване на справки на засегнати лица.

В хода на обработката по поръчка Възложителят формално и съдържателно контролира резултатите от работата на Изпълнителя. Спазването на взетите от Изпълнителя технически и организационно мерки се проверява редовно. За тази цел най-вече се ползва представянето на актуалните удостоверения или подходящите сертификати, респективно удостоверения от проведени одити на ИТ сигурността или защитата на данните. Ако бъдат използвани подизпълнители, в Договора се определя, че те съответно ще бъдат контролирани.

6. Гарантиране на натоварване на системата

Облачната инфраструктура на AWS е създадена като една от най-гъвкавите и сигурни среди за облачен компютинг. Тя е разработена за оптимална достъпност при пълно отделяне на клиента. Тя доставя екстремно мащабируема и много сигурна за работа платформа, която дава възможност на клиентите по целия свят при нужда бързо и сигурно да извадят приложения и съдържания. Услугите AWS са дотолкова независими от съдържанието, доколкото предлагат на

всички клиенти същото високо ниво на сигурност, независимо от вида на съдържанията или от географския регион, в който са записани съдържанията.

Центрове за данни на AWS с максимално ниво на сигурност от световна класа използват мерки за електронен надзор на състоянието на техниката и многостепенни системи за контрол на достъпа. В центровете за данни денонощно има обучен персонал по сигурността и достъпът е строго гарантиран на принципа на минималните права и само за целите на системната администрация.

7. Процедури за възстановяване на достъпността до лични данни след физически или технически инцидент

Центровете за данни на AWS са изградени в клъстери в различни региони по света. Всички центрове за данни са онлайн и обслужват клиенти; никой център за данни не е изключен. При неизправност автоматични процеси прехвърлят трафика на клиентски данни далеч от засегнатите области. Основните приложения са предоставени в конфигурация N+1, така че в случай на неизправност в центъра за данни да има достатъчно наличен капацитет, за да се разпредели трафикът на данни по останалите местоположения, без да бъдат натоварени.

AWS предлага гъвкавост за позициониране на инстанции и записване на данни в рамките на множество географски региони, както и чрез множество зони на наличност в рамките на отделните региони. Всяка зона на наличност се разработва като независима зона по отношение на неизправността. Това означава, че зоните на наличност в рамките на типичен градски регион са физически разпредени и се намират например в области с нисък риск от наводнение (според региона има различни категории на зоните с риск от наводнение). Допълнително към самостоятелното непрекъснато електрозахранване и генераторите за аварийно захранване на място всички зони на наличност са захранени от различни електрически мрежи от независими доставчици на електричество, за да се минимизират местата с единични грешки. Всички зони на наличност са с резервна връзка с множество доставчици Tier-1-Transit.

Екипът на Amazon за управление на инциденти прилага обичайните за бранша методи за диагностика, за да ускори отстраняването на критични за фирмата инциденти. Фирменият персонал е на денонощно разположение, седем дни в седмицата и 365 дни в годината, за да разпознае инцидентите и да управлява техните влияния и отстраняването им.

8. Процедури по редовна проверка, преценка и оценка на ефективността на техническите и организационните мерки

Наличните във фирмата предписания и указания, респективно имплементираните стандарти за информационна сигурност, се прилагат и във връзка с въвеждането и експлоатацията на платформата RIO. Фирмените функции за защита на данните и информационна сигурност са налични (лице, упълномощено за защита на личните данни, и служител по информационната сигурност). Служителите са задължени да пазят в тайна данните и са информирани за мерките за сигурността на данните, респективно ИТ мерките за сигурност, чрез брошури, флаери, интранет указания и др.

Вътрешните процеси във връзка със спазването на техническите и организационните мерки за сигурност на данните се проверяват чрез ревизии, информационна сигурност и защита на данните.

Процесите по обработка и мерките за сигурност на данните се документират в списък с дейностите по обработка. Редовно се извършва проверка (вътрешна и външна) на ефективността на мерките.