

Ordrebehandlingsaftale

mellem

..... *Kundenummer*

..... *Firmanavn*

..... *Gade/vej, nr.*

..... *Postnummer, by*

..... *Land*

- efterfølgende „ordregiver“-

og

HELLA Gutmann Solutions GmbH

Am Krebsbach 2

D-79241 Ihringen

Tyskland

- efterfølgende „ordretager“-

- Ordretager og ordregiver sammen „parterne“ eller alene „part“

Fortale

Ordretageren udvikler og sælger elektroniske diagnostiske løsninger til motorkøretøjer. Han modtager via en elektronisk grænseflade data vedrørende køretøjer fra ordregiverens firma. Blandt disse data befinder der sig også data, som i henhold til databeskyttelsesforordningen („GDPR“) er personlige data, f.eks. køretøjets indregistrerings- og identifikationsnummer. For at regulere håndteringen af disse personlige data, indgår parterne efterfølgende aftaler.

1. Aftalens formål, omfang og varighed

- 1.1. Ordregiveren anviser ordretageren med behandlingen og brugen af de i punkt 1.2. anførte data under hensyntagen til de i denne aftale fastlagte rettigheder og forpligtelser.
- 1.2. De af denne aftale omfattede data er de personlige data, som ordretageren modtager i forbindelse med reparation/vedligeholdelse af motorkøretøjer fra ordregiverens firma, køretøjernes indregistrerings- og identifikationsnumre (FIN/VIN). Disse data betegnes efterfølgende som „**aftaledata**“.
- 1.3. I henhold til den aktuelle status indeholder disse aftaledata følgende typer data:
 - FIN/VIN
 - indregistreringsnummer

Desuden indeholde aftaledataene ved brug af HGS Data, Tolerance Data, NF Data, ACREP, Dabeko, Dacarsa, Toyota (Tolerance), MekoTolerance, DiagnosES:

 - navn, adresse, e-mailadresse og telefonnummer på køretøjets ejer
- 1.4. Ordretageren registrerer, gemmer og behandler aftaledataene. Denne behandling af aftaledataene sker udelukkende til forberedelse og understøttelse af ordregiverens vedligeholdelses- og reparationsarbejder som led i driften.
- 1.5. Ordretageren vil gemme disse aftaledata indtil aftaleforholdets udløb (punkt 12.) eller indtil en tidligere anvisning om sletning fra ordregiveren. En længere lagring er tilladt, hvis en lovmæssig opbevaringsbestemmelse kræver dette.
- 1.6. Berørt af den førnævnte overførsel og behandling af aftaledataene er
 - ordregiverens kunder (herunder også forbrugere),
 - køretøjernes ejere,
 - ordregiverens medarbejdere

2. Tekniske og organisatoriske foranstaltninger vedrørende datasikkerhed

- 2.1. Ordretageren forpligter sig til, at sikre aftaledataene effektivt i henhold til det aktuelle tekniske niveau mod uautoriseret adgang, ændring, ødelæggelse eller tab, utilladelig overførsel, anden uautoriseret behandling og misbrug og til iht. stk. 32 GDPR at træffe de nødvendige tekniske og organisatoriske foranstaltninger („TOMs“). Med disse TOMS skal det garanteres, at aftaledataene bliver sikret tilstrækkelig samt beskyttes mod misbrug, tab og uautoriseret behandling via tredjepart.
- 2.2. Den aktuelle status for de af ordretagerens trufne TOMs er opført i **bilag 1**. Ordretageren skal tilpasse hans TOMs i løbet af aftaleforholdet, hvis de trufne foranstaltninger ikke mere svarer til det aktuelle tekniske niveau og/eller tilpasninger på grund af den organisatoriske udvikling bliver nødvendige, såfremt implementeringsomkostningerne står i et rimeligt forhold til risikoen for de pågældende personers rettigheder

og friheder. Sikkerhedsniveauet af de i **bilag 1** opførte TOMs må derved ikke underkrides. Ordretageren skal dokumentere ændringer af disse TOMs.

2.3. I tilfælde af punkt 6.3. og 6.4. (sikkerhedsbrud) skal ordretageren tilpasse hans TOMS i henhold til punkt 2.2. i denne aftale, såfremt dette er egnet og nødvendigt til en fremtidig undgåelse af lignende overtrædelser. Parterne skal desuden træffe passende foranstaltninger til reducere af negative konsekvenser for de berørte.

3. Ordregiverens rettigheder og pligter, kontrolforanstaltninger

3.1. For vurderingen af behandlingens pålidelighed iht. art. 6 stk. 1 i GDPR samt for varetagelsen af de pågældende personers rettigheder iht. art. 12 til 22 GDPR er ordregiveren alene ansvarlig.

3.2. Ordregiveren er via inspektioner på stedet samt iht. punkt 3.3 inden starten af databehandlingen og derefter med jævne mellemrum efter aftale berettiget til at overbevise sig om overholdelsen af de hos ordretageren iht. punkt 2 i denne aftale trufne TOMs. Derved er ordregiveren ikke berettiget til selv at udføre disse inspektioner. I stedet skal han anvise sagkyndige med en sådan inspektion, som over for ordretageren skal forsikre, at de udelukkende kontrollerer overholdelsen af de i art. 28 i GDPR fastsatte forpligtelser og at de kun stiller ordregiveren disse resultater til rådighed, altså at de i særdeleshed ikke afslører forretningshemmeligheder fra ordretageren over for ordregiveren.

3.3. Desuden er ordregiveren berettigede til af ordretageren at få oplysning og informationer om realiseringen af disse TOMs iht. punkt 2 samt om overholdelsen af alle andre i art. 28 i GDPR fastsatte forpligtelser. Et sådan forlangende kan ordretageren selv opfylde eller få opfyldt via tredjepart, idet han f.eks.:

3.3.1. selv giver oplysning om realiseringen af disse TOMs;

3.3.2. fremlægger en attest, en rapport eller et rapportuddrag fra en uafhængig instans (f.eks. en sagkyndig).

3.4. De omkostninger, som i givet fald opstår som led i disse kontroller iht. punkt 3.2. til 3.3. i denne aftale, især grundet en bestilling hos tredjepart, påhviler ordregiveren, såfremt ordregiveren selv bestiller denne tredjepart eller forlanger bestillingen af ordretageren.

3.5. Ordregiveren skal omgående informere ordretageren, hvis han konstaterer fejl eller uregelmæssigheder ved kontrollen af disse TOMs.

4. Ordretagerens rettigheder og pligter

4.1. Ordretageren og enhver ham underordnet person, der har adgang til aftaledataene, behandler udelukkende aftaledataene på ordregiverens vegne, i henhold til dennes anvisninger og som led i denne aftales formål, såfremt han ikke grundet lovgivningen i Den Europæiske Union eller medlemslandene, som aftalepartneren er underlagt, er forpligtet til en anden behandling. I et sådant tilfælde informerer ordretageren ordregiveren om disse retslige krav inden behandlingen, såfremt den pågældende lovgivning ikke forbyder en sådan information grundet en vigtig offentlig interesse.

- 4.2. Udover som anvisning af ordregiveren må ordretageren hverken indsamle, behandle eller bruge aftaledataene til egne eller tredjeparters formål.
- 4.3. Ordretageren må kun berigtige, slette eller spærre aftaledataene efter anvisning fra ordregiveren, såfremt ordretagerens berettigede interesser ikke udelukker dette.
- 4.4. Ordretageren udfærdige ikke kopier og duplikater af aftaledataene uden tilladelse fra ordregiveren. Undtaget er sikkerhedskopier, såfremt disse er nødvendige til sikring af en korrekt databehandling, og data som er nødvendige til overholdelse af lovplichtige opbevaringspligter.
- 4.5. Ordretageren er forpligtet til omgående at lede alle forespørgsler fra tredjeparter vedrørende aftaledataene videre til ordregiveren. Han er uden en skriftlig tilladelse fra ordregiveren ikke autoriseret til at give vedkommende eller andre tredjeparter oplysning om aftaledataene.
- 4.6. Giver man ordretageren adgang til ordregiverens EDB-anlæg, må denne adgang kun bruges til opfyldelse af pligterne fra denne aftale.
- 4.7. Ordretageren skal i betragtning af behandlingens art og i henhold til hans muligheder med egnede TOMs understøtte ordregiveren i dennes pligt om at efterkomme besvarelse af anmodninger om varetagelse af de i kapitel III i GDPR nævnte personlige rettigheder. Desuden skal han under hensyntagen til behandlingens art og med de informationer, der står ham til rådighed understøtte ordregiveren ved overholdelsen af de i art. 32 til 36 i GDPR nævnte pligter. Ordregiveren skal erstatte ordretageren de derved opståede omkostninger. Disse bestemmer parterne med € 50,00 / time, i givet fald plus moms.

5. Databeskyttelsesansvarlig

- 5.1. Hos ordretageren er Eike Westermann (dataprivacy@hella.com) udpeget som databeskyttelsesansvarlig.
- 5.2. Ordregiveren skal omgående informeres om en ændring af den databeskyttelsesansvarlige.

6. Oplysningspligter

- 6.1. Ordretageren skal omgående gøre ordregiveren opmærksom på, hvis en anvisning fra denne efter hans opfattelse strider mod GDPR eller andre databeskyttelsesbestemmelser i Den Europæiske Union eller medlemsstaterne. Ordretageren må udsætte udførelsen af den tilsvarende anvisning, indtil ordretageren er blevet informeret om ordregiverens kontrol og kontrolresultater. Hvis ordregiverens kontrol viser, at der virkelig foreligger en overtrædelse af de relevante databeskyttelsesbestemmelser, vil ordretageren ikke udføre anvisningen. Såfremt der heller ikke efter denne kontrol gennem ordregiveren er enighed mellem parterne om anvisningens forenelighed med GDPR eller andre databeskyttelsesbestemmelser fra Den Europæiske Union eller medlemsstaterne, skal parterne informere den ansvarlige tilsynsmyndighed og iht. art. 58 stk. 2 lit. a) i GDPR indhente dennes afgørelse.
- 6.2. Bliver ordretageren bekendt med en overtrædelse af beskyttelsen af aftaledataene, skal han omgående informere den ansvarlige om dette. Overtrædelsen af beskyttelsen af aftaledataene er så ordretageren bekendt, når han på den måde opnår til-

strækkelig kendskab, som tillader ham at foretage en meningsfuld meddelelse i henhold til bestemmelserne i bestemmelserne i GDPR.

6.3. Punkt. 6.2. gælder tilsvarende, hvis ordretageren bliver bekendt med forstyrrelser i behandlings- eller driften eller andre overtrædelser af bestemmelser til beskyttelse af aftaledataene.

6.4. Ordretageren skal omgående informere ordregiveren om kontrolhandlinger og foranstaltninger fra tilsynsmyndigheden, såfremt disse vedrører aftaledataene. Dette gælder også, såfremt en ansvarlig myndighed efterforsker hos ordretageren. Ordretageren efterkommer myndighedsmæssige bestemmelser i forbindelse med aftaledata.

7. Anvisningsbemyndigelse / omfang

7.1. Anvisninger skal gives i tekstform (skriftligt eller pr. e-mail).

7.2. Ordretageren skal dokumentere anvisningerne fra den ansvarlige på en egnet måde.

8. Forpligtelse til datafortrolighed

8.1. Ordretageren forpligter sig til overholdelse af datafortroligheden ved behandlingen af aftaledataene.

8.2. I den forbindelse skal ordretageren forpligte de med udførelse af arbejderne betroede medarbejdere til fortrolighed. Desuden skal ordretageren informere disse medarbejdere om den eksisterende anvisnings- og formålsbestemmelse.

8.3. Datafortroligheden fortsætter også efter aftalens udløb.

9. Grænseoverskridende behandling

Tilvejebringelsen af den aftalte databehandling finder udelukkende sted i en medlemsstat i Den Europæiske Union eller i en stat, der er omfattet af aftalen om det europæiske økonomiske samarbejdsområde. Aftaledataene skal lagres inden for Den Europæiske Union eller det europæiske økonomiske samarbejdsområde. Enhver behandling af aftaledata i et tredjeland, herunder hentning af data fra et sådant tredjeland (f.eks. via kundeservice, helpdesk etc.), kræver en forudgående accept fra ordregiveren i tekstform og må kun ske, hvis de særlige betingelse i art. 44 ff. i GDPR er opfyldt. Ordregiveren skal acceptere dette, såfremt de lovbestemte betingelser overholdes. Dette gælder også, hvis der gøres brug af underleverandører i tredjelande. Til sikring af et passende databeskyttelsesniveau er parterne forpligtet til at anvende standardkontraktklausuler fra den Europæiske Kommission, så snart disse foreligger. Hvis disse klausuler er aftalt mellem ordretager og underleverandør, kræves der ingen accept fra ordregiveren.

10. Underleverandører

10.1. Ordretageren er berettiget til at overdrage databehandlingen til underleverandører. I den forbindelse skal de kontraktmæssige aftaler med en underleverandør udformes således, at de svarer til databeskyttelsesbestemmelserne i aftaleforholdet

mellem ordregiver og ordretager. En liste over de p.t. benyttede underleverandører er vedlagt denne aftale som **bilag 2**.

- 10.2. Ordretageren skal informere ordregiveren rettidigt forud om enhver påtænkt ændring vedrørende inddragelse eller udskiftning af underleverandører i tekstform (skriftligt eller pr. e-mail). Ordregiveren er berettigede til inden for to uger at gøre indsigelse mod sådanne ændringer fra modtagelsen af informationen i tekstform (skriftligt eller pr. e-mail).
- 10.3. Ordretageren sørger for, at hans underleverandør accepterer de i punkt 3.2. og 3.3. i denne aftale anførte kontrolrettigheder. Ved hjælp af disse skal han i særdeleshed sørge for, at underleverandøren giver tilstrækkelige garantier for at de egnede tekniske og organisatoriske foranstaltninger udføres således hos underleverandøren, at behandlingen sker tilsvarende kravene i GDPR. Ordretageren skal dokumentere resultaterne af kontrollerne og gøre disse tilgængelige for ordregiveren, hvis denne skulle forlange dette.
- 10.4. Aftaler med underleverandører skal udarbejdes i tekstform (skriftligt eller pr. e-mail).

11. Ejerskab af datamedier, returnering af data og datamedier, sletning

- 11.1. Af ordregiveren overdragede datamedier med gemte aftaledata, tilhører ordregiveren.
- 11.2. Efter afslutning af de aftalemæssige arbejder (eller før efter anmodning fra ordregiveren) skal ordretageren slette de hos ham eksisterende aftaledata fuldstændigt, såfremt dette ikke strider mod lovbestemte opbevaringspligter.
- 11.3. Sletningen skal protokolleres med dato og bekræftes af ordregiveren i tekstform (skriftligt eller pr. e-mail) på dennes anmodning.

12. Varighed

- 12.1. Denne aftale træder i kraft ved undertegnelsen af parterne og indgås på ubestemt tid.
- 12.2. Aftalen kan opsiges ordentligt af begge parter ved overholdelse af en frist på to uger. Dette gælder ikke så længe ordretageren er forpligtet til at behandle aftaledata for ordregiveren fra en anden aftale. I dette tilfælde begynder den to ugers opsigelsesfrist først ved udløb af den anden aftale.
- 12.3. Aftalen kan af begge parter opsiges uden overholdelse af en opsigelsesfrist, hvis der foreligger en vigtig grund. En vigtig grund foreligger, hvis det med rimelighed ikke kan forlanges at den opsigende part under hensyntagen til alle omstændigheder ved det enkelte tilfælde og under overvejelse af begge siders interesser fortsætter aftaleforholdet indtil den aftalte afslutning eller indtil udløbet af en opsigelsesfrist. Dette er især tilfældet, hvis en af parterne begår en alvorlig overtrædelse af bestemmelserne i denne aftale eller af bestemmelserne i GDPR.
- 12.4. Opsigelser skal ske skriftlig iht. § 126 BGB.

13. Gældende lovgivning / Værneting / Salvatorisk klausul

13.1. Parterne aftaler anvendelse af tysk lovgivning med undtagelse af lovkonfliktreglerne. Værneting for alle stridigheder fra eller i forbindelse med denne aftale er ordretagerens sæde.

13.2. Skulle enkelte bestemmelser i denne aftale være ugyldige eller uigennemførlige eller blive ugyldige eller uigennemførlige efter aftalens indgåelse, forbliver gyldigheden af den øvrige bestemmelser i aftalen upåvirket af dette. I stedet for den ugyldige eller uigennemførlige bestemmelse skal den gyldige eller gennemførlige bestemmelse anvendes, hvis virkningerne kommer det økonomiske mål kommer nærmest, som aftaleparterne forfulgte med den ugyldige eller uigennemførlige bestemmelse.

Sted, dato

Ihringen den 23. maj 2018

.....
.....

Underskrift ordregiver
(Stedfortræder 1)

(Managing Director)

.....

Rolf Kunold

Navn med blokbogstaver

- Bilag 1 -

Tekniske og organisatoriske foranstaltninger

De efterfølgende tekniske og organisatoriske foranstaltninger skal defineres detaljeret og navngives specifikt.

Er følsomme eller særlige typer personlige data omfattet af ordren (f.eks. oplysninger om fagforeningsmedlemskab eller sundhed), skal der træffes særlige beskyttelsesforanstaltninger. Disse skal nævnes og forklares specielt.

De følgende foranstaltninger er minimumskrav. De skal til enhver tid sikres af ordretageren:

1. Adgangskontrol

Uautoriserede skal forbydes adgang (i rummelig hensigt) til EDB-anlæg, hvor de personlige data behandles eller bruges.

Tekniske og organisatoriske foranstaltninger vedrørende adgangskontrol:

- ID-kortlæser, chipkort;
- Beskyttelsesforanstaltninger mod tyveri, manipulation og skader, på de til databehandlingen anvendte apparater; f.eks. adgangsaunorisationskoncept til server, USV og klimatisering af serverrum
- Forskellige sikkerhedszoner på fabriksarealet;
- Protokollering af personalet på stedet;
- Kontrolleret udlevering af nøgler (herunder adgangsområder);
- Dørsikkerhedssystem (elektrisk døråbner etc.);
- Vagtjeneste, portner;
- Regler for adgang af eksterne parter;
- Gennemgangsspærringer (f.eks. drejekors);
- Overvågningsanlæg, f.eks. alarmanlæg

2. Adgangskontrol

Det skal forhindres, at EDB-systemer kan bruges af uautoriserede.

Tekniske (kodeord- / password beskyttelse) og organisatoriske (brugerstamdata) foranstaltninger hvad angår brugeridentifikation og autentificering:

- Autorisationskoncept og indførelse af differentierede adgangsniveauer (system);
- Individuelt bruger-ID;
- Password-metode (bl.a. specialtegn, minimal længde, password skal ændres regelmæssigt);
- Proces designet og implementeret, som sikrer, at alle adgangsrettigheder straks tilbagekaldes, når en medarbejder forlader ordretagerens virksomhed;
- Firewall;
- Kryptering af datamedier i henhold til en acceptabel brugspolitik Ordning til brug / bortskaffelse af datamedier (f.eks. USB, eksterne harddiske);
- Regler for adgang af eksterne parter.

3. Adgangskontrol

Det skal sikres, at personer, der er autoriseret til brug af et EDB-system udelukkende har adgang til data tilsvarende deres adgangsrettigheder, og at personlige data ved behandling, brug og efter lagringen ikke uautoriseret kan læses, kopieres, ændres eller slettes.

Foranstaltninger til udvikling af autorisationskonceptet og adgangsrettigheder samt deres overvågning og protokollering:

- Autorisationskoncept og realisering af differentierede adgangsniveauer (data);
- Alle server bliver hostet i sikre datacentre, som hvad angår deres sikkerhed regelmæssigt bliver testet;
- Det er ikke muligt, at installere ukendt / ikke autoriseret software på hardwaren hos ordretageren;

4. Videregivelseskontrol

Det skal sikres, at personlige data ved den elektroniske overførsel eller under deres transport eller lagring på datamedier ikke kan læses, kopieres, ændres eller slettes uautoriseret.

Foranstaltninger ved overførsel, transport eller lagring på datamedier (manuel eller elektronisk) same ved den senere kontrol:

- Kryptering, tunnelforbindelse (VPN = Virtual Private Network);
- Protokollering af overførselstype / overførte data / modtager transportbeskyttelse.

5. Indtastningskontrol

Det skal sikres, at man senere kan se, om og hvem der har indtastet, ændret eller slettet personlige data i EDB-systemer

Foranstaltninger til senere kontrol af, om og hvem der har indtastet, ændret eller slettet data:

- Protokollering af systemaktiviteten (Læse, ændre, ikke autoriserede adgangsforsøg, regelmæssig protokolanalyse / speciel-analyse, hvis nødvendigt);
- Regelmæssig og systematisk analysering af protokolleringen;

6. Ordrekontrol

Det skal sikres, at de personlige data, der behandles i ordren, kun behandles tilsvarende anvisningerne fra ordregiveren.

Foranstaltninger til afgrænsning af kompetencer mellem ordregiver og ordretager:

- Medarbejderne skal forpligtes separat til hemmeligholdelse af de overførte kundedata;
- Kundedataene skal mindst behandles med den samme påpasselighed som ordretagerens egne "fortrolige" data ;

- Styring af aftalens udførelse (kontrol / auditering af underleverandører via ordretageren, ordregiveren får resultaterne af ordretagerens selvevaluering).

7. Tilgængelighedskontrol

Ordretageren skal sikre, at personlige data er beskyttet mod tilfældig ødelæggelse eller tab.

Foranstaltninger til datasikring (ødelæggelse / tab):

- Backup-metode;
- Separat opbevaring;
- Spejling af harddiske (f.eks. RAID-metode);
- Afbrydelsesfri strømforsyning (ASF);
- Koncept til arkivering af data;
- Regelmæssig kontrol af systemets status (monitoring);
- Virusbeskyttelse;

8. Adskillelseskontrol

Det skal sikres, at data, der er indsamlet til forskellige formål også behandles separat.

Foranstaltninger til separat behandling (lagring, ændring, sletning, overførsel) af data til forskellige formål:

- Adskillelse af realtid- og testsystem;
- Dokumenteret funktionsadskillelse.

- Bilag 2 -

Løbende nr.	Firmanavn	Adresse	Formålet med underentrepriser:
1	Asanetwork GmbH	Vennhauser Allee 265 40627 Düsseldorf Tyskland	Til sammenknytning med anden software på værkstedet med diagnoseapparaterne
2	Hella Gutmann Solutions A/S	Lundborgvej 10, 8800 Viborg, Danmark	Til korrekt valg af køretøj
3	TecAlliance GmbH	Steinheilstraße 10 85737 Ismaning Tyskland	Til korrekt identifikation af køretøjer i Østrig, Schweiz, Tyskland, Frankrig og Nederlandene
4	Bisnode Danmark a/s	Gyngemose Parkvej 50, 8 2860 Søborg Danmark	Til korrekt identifikation af køretøjer i Finland, Norge og Sverige
5	FTZ Autodele & Værktøj A/S	Hvidkærvej 21 5250 Odense SV Danmark	Til korrekt identifikation af køretøjer in Danmark og hosting service
6	Microsoft Danmark ApS	Kanalvej 7 2800 Kongens Lyngby Danmark	Hosting service