



Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend

MLU B.V.
t.a.v. de heer [VERTROUWELIJK]
Postbus 40198
8004 DD ZWOLLE

Datum
1 april 2026

Ons kenmerk
2025-005323

Contactpersoon
[VERTROUWELIJK]

Onderwerp

Besluit tot het opleggen van een bestuurlijke boete voor het overtreden van de Algemene verordening gegevensbescherming

Geachte heer [VERTROUWELIJK],

De Autoriteit Persoonsgegevens (hierna: AP) heeft besloten om aan MLU B.V. als rechtsverkrijger van alle rechten en plichten van de inmiddels ontbonden onderneming Ridetech International B.V. (hierna: Ridetech) een bestuurlijke boete van € 100.000.000 op te leggen. Deze boete wordt opgelegd vanwege de schending van de Algemene verordening gegevensbescherming (AVG). Ridetech heeft zich schuldig gemaakt aan de doorgifte van persoonsgegevens van betrokkenen uit Finland en Noorwegen naar ontvangers in Rusland zonder dat Ridetech heeft aangetoond dat zij daarvoor passende waarborgen heeft getroffen. Dit levert een overtreding op van artikelen 44 en 46 AVG in samenhang met artikel 5, eerste lid, onder a en tweede lid, AVG. De overtreding ving aan op 23 mei 2022 en duurt nog immer voort.

De AP is van mening dat het opleggen van een bestuurlijke boete aan MLU B.V. niet alleen gepast is, maar ook noodzakelijk. De AP heeft namelijk geconstateerd dat MLU B.V. het beoogde belang van de continuïteit van het hoge niveau van de bescherming van de AVG bij doorgifte van persoonsgegevens naar een derde land, niet heeft gewaarborgd. De AP vindt dat ernstig en is om die reden tot handhaving jegens MLU B.V. overgegaan.

Onderdeel van dit handhavend optreden is dat de AP aan MLU B.V. een verbod oplegt tot verwerking van persoonsgegevens. Dat betekent dat MLU B.V. moet stoppen met de doorgifte van persoonsgegevens van Noorse en Finse gebruikers van de Yango-app aan ontvangers in Rusland.

Datum
1 april 2026

Ons kenmerk
2025-005323

In dit besluit worden de bestuurlijke sancties toegelicht. Hiertoe wordt achtereenvolgens ingegaan op de feiten, de zienswijze, de vastgestelde overtreding, de hoogte van de boete en het verwerkingsverbod. Tot slot volgt het dictum.

1. Aanleiding onderzoek

1. De AP heeft in 2021 en 2022 van de Finse privacytoezichthouder, *Tietosuoja-valtuutetun toimisto* (hierna: de Finse privacytoezichthouder) een signaal ontvangen over Ridetech. Dit signaal ging over een mogelijke doorgifte van persoonsgegevens van betrokkenen uit de Europese Economische Ruimte (hierna: EER) naar Rusland, door Ridetech, zonder dat een geldig mechanisme van toepassing was voor internationale doorgifte van persoonsgegevens in de zin van de AVG. In het bijzonder ging het signaal over de 'ride-hailing' apps 'Yango for users' en 'Yango Pro for drivers' (hierna gezamenlijk: Yango-app).¹ De Yango-app is een platform waarop zelfstandige chauffeurs worden gekoppeld aan klanten die een taxirit willen boeken.
2. Ridetech is een in Amsterdam gevestigde onderneming die de Yango-app aanbiedt binnen de EER aan betrokkenen in Finland en Noorwegen. In het kader van de dienstverlening van de Yango-app geeft Ridetech (persoons)gegevens vanuit de EER door aan Yandex.Taxi LLC en Yandex LLC. Beide ondernemingen zijn gevestigd in Rusland. Ridetech, Yandex.Taxi LLC en Yandex LLC zijn ondernemingen die tot hetzelfde concern behoren.
3. Op 4 augustus 2023 heeft de Finse privacytoezichthouder in een spoedprocedure een besluit genomen (artikel 66 AVG). Dit besluit bevatte voorlopige maatregelen die geldig waren van 1 september 2023 tot 30 november 2023. In dat besluit heeft de Finse privacytoezichthouder, onder meer, geoordeeld dat de doorgifte van persoonsgegevens vanuit Finland naar Rusland in het geval van de Yango-app in strijd is met artikelen 44 en 46 AVG. De Finse privacytoezichthouder heeft gelet daarop de doorgifte verboden op grond van artikel 58, tweede lid, onder f, AVG.²
4. Ook de Noorse privacytoezichthouder, *Datatilsynet* (hierna: de Noorse privacytoezichthouder) heeft een spoedprocedure gestart tegen Ridetech wegens de doorgifte van persoonsgegevens vanuit Noorwegen naar Rusland. Dit heeft zij op 7 augustus 2023 medegedeeld aan Ridetech, Yandex LLC en Yango Norway AS.³
5. Op 30 augustus 2023 heeft de Finse privacytoezichthouder het besluit van 4 augustus 2023 geschorst. De Noorse privacytoezichthouder heeft op 31 augustus 2023 aan Ridetech, Yandex LLC en Yango Norway AS

¹ Onderzoeksrapport, p 7.

² Dossierstuk 12 bij het onderzoeksrapport.

³ Dossierstuk 13 bij het onderzoeksrapport.

Datum
1 april 2026

Ons kenmerk
2025-005323

laten weten dat zij geen voorlopige maatregelen zou treffen, maar wel verder onderzoek zou starten naar de verwerkingen van persoonsgegevens.⁴

6. Op 5 december 2023 heeft de AP een onderzoek ingesteld naar de doorgifte door Ridetech van persoonsgegevens naar Rusland in het kader van eerdergenoemde dienstverlening van Ridetech. De Finse en Noorse privacytoezichthouders hebben zich op 18 december 2023 aangesloten bij dit AP-onderzoek.
7. Het doel van dit gezamenlijke onderzoek was om vast te stellen of Ridetech in de periode van 23 mei 2022 tot heden voldoet aan de AVG-regels omtrent de internationale doorgifte van persoonsgegevens vanuit de EER naar Rusland. De afdeling Internationaal Onderzoek van de AP heeft daarom onderzocht of persoonsgegevens van de chauffeurs en klanten die de Yango-app gebruiken (hierna gezamenlijk: gebruikers) uit de EER worden doorgegeven naar Rusland. Ook heeft de afdeling Internationaal Onderzoek van de AP onderzocht of Ridetech passende waarborgen in de zin van artikel 46 AVG heeft getroffen voor de doorgifte van persoonsgegevens naar Rusland.

2. Bevindingen onderzoeksrapport en procesverloop

2.1 Procesverloop

8. De afdeling Internationaal Onderzoek van de AP heeft de bevindingen van het onderzoek opgeschreven in een rapport van 2 april 2025.⁵ De AP heeft bij brief van 8 april 2025 aan Ridetech medegedeeld voornemens te zijn handhavingsmaatregelen te treffen. De AP heeft Ridetech in de gelegenheid gesteld om een zienswijze te geven op het voornemen tot handhaving en het daaraan ten grondslag liggende rapport. Ridetech heeft op 10 juni 2025 haar zienswijze op het rapport gegeven. Op 16 juni 2025 heeft Ridetech haar zienswijze mondeling toegelicht.
9. De directeur van Ridetech heeft de AP bij brief van 28 oktober 2025 geïnformeerd dat Ridetech per 24 oktober 2025 is ontbonden en dat haar moederonderneming, MLU B.V. per die datum alle rechten en plichten van Ridetech zal overnemen.⁶ Daarnaast heeft de directeur van Ridetech medegedeeld dat alle diensten van de Yango-app in Noorwegen en Finland zijn gestaakt. Desgevraagd hebben de Noorse en Finse privacytoezichthouders vastgesteld dat de Noorse en Finse aanbieders van de Yango-app nog immer ingeschreven staan in het Handelsregister van beide landen en dat de diensten van de Yango-app thans nog steeds worden aangeboden.⁷
10. In het hiernavolgende worden de belangrijkste bevindingen van het onderzoeksrapport samengevat.

⁴ Dossierstuk 59 bij het onderzoeksrapport.

⁵ Het onderzoeksrapport is op 8 april 2025 aan Ridetech verzonden.

⁶ Bijlage 2 bij dit besluit.

⁷ Bijlage 3 bij dit besluit.

Datum
1 april 2026

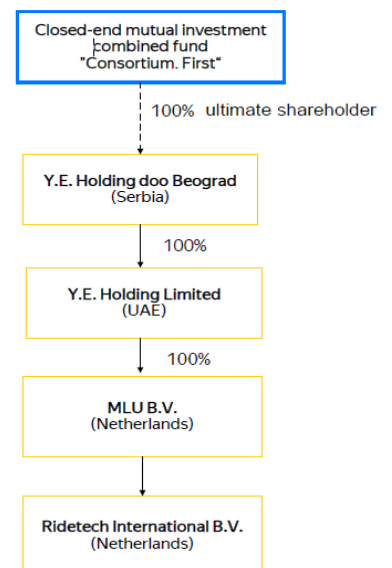
Ons kenmerk
2025-005323

2.2 Verwerkingsverantwoordelijke

11. In de privacyverklaring van Ridetech staat dat zij verwerkingsverantwoordelijke is voor verwerkingen van persoonsgegevens van gebruikers van de Yango-app op het EER-grondgebied. Ridetech was gevestigd in Amsterdam totdat zij op 24 oktober 2025 werd ontbonden.⁸ Ridetech maakt onderdeel uit van een grote concernstructuur. Voor een betere leesbaarheid van dit besluit zal de AP de naam 'Ridetech', blijven gebruiken.
12. Ridetech was, totdat zij op 24 oktober 2025 werd ontbonden, een dochteronderneming van MLU B.V. die op haar beurt een dochteronderneming was van Yandex N.V. Holding Company.⁹ MLU B.V. is, na een herstructurering in februari 2024, een dochteronderneming geworden van Y.E. Holding Limited, gevestigd in de Verenigde Arabische Emiraten.¹⁰ Y.E. Holding Limited is per 24 juli 2024 een dochteronderneming van Y.E. Holding doo Beograd, gevestigd in Servië. Consortium.First is de enige aandeelhouder van Y.E. Holding doo Beograd. Ter illustratie is de volgende concernstructuur¹¹ opgenomen:

Yandex

Corporate structure as of July 24, 2024:
Ridetech International B.V.



⁸ Dossierstuk 134 bij het onderzoeksrapport.

⁹ Dossierstuk 29 bij het onderzoeksrapport.

¹⁰ Dossierstukken 81 en 111 bij het onderzoeksrapport.

¹¹ Dossierstuk 112 bij het onderzoeksrapport.

Datum
1 april 2026

Ons kenmerk
2025-005323

13. Yandex.Taxi LLC is gevestigd in Rusland. Tot 15 juli 2024 was Yandex.Taxi LLC een dochteronderneming van Ridetech International B.V. Na 15 juli 2024 is Yandex.Taxi LLC een dochteronderneming van Yandex.Technologies LLC, gevestigd in Rusland.¹²

Na wijziging van het business model (1 maart 2025)

14. Op 27 februari 2025 heeft Ridetech de AP op de hoogte gebracht van een voorgenomen wijziging in het businessmodel van de Yango-app.¹³ Met ingang van 1 maart 2025 wordt de Yango-app aangeboden via een franchise model, waarbij de dienstverlening per land wordt geregeld. Met ingang van 1 maart 2025 verleent de Finse onderneming CABS TEK OY de diensten van de Yango-app aan consumenten in Finland. Met ingang van 1 maart 2025 verleent de Noorse onderneming SENTRAL OSLO CABS AS de diensten van de Yango-app aan consumenten in Noorwegen.¹⁴
15. Vanaf 7 maart 2025 beschouwt Ridetech zich samen met de Finse en Noorse ondernemingen als gezamenlijk verwerkingsverantwoordelijken voor verwerkingsactiviteiten binnen de EER.¹⁵

2.3 Verwerking van persoonsgegevens

16. De diensten van de Yango-app worden verleend via twee apps voor mobiele telefoons, 'Yango for users' en 'Yango Pro for drivers'. Klanten kunnen via 'Yango for users' taxiriten aanvragen en chauffeurs kunnen via 'Yango Pro for drivers' de aanvragen accepteren.
17. Klanten moeten voor het gebruik van de Yango-app eerst een geldig telefoonnummer opgeven. Ook vraagt Ridetech om contactgegevens en andere gegevens. Dit is afhankelijk van de juridische regels die gelden in het betreffende land. Zo is het in Noorwegen niet mogelijk om een taxi te bestellen zonder registratie van een geldig bankrekeningnummer. Voor het registreren van klanten gebruikte Ridetech aanvankelijk 'Yandex ID'.¹⁶ Yandex ID geeft gebruikers ervan toegang tot alle diensten van Yandex, zoals Yandex Pay. De diensten van Yandex ID worden aangeboden door de in Rusland gevestigde Yandex LLC.¹⁷ Ridetech maakt in ieder geval per 19 maart 2025 geen gebruik meer van Yandex ID.¹⁸
18. Na het afronden van het registratieproces kunnen klanten een taxirit aanvragen. Dat doen zij door het adres van het ophaalpunt door te geven. Klanten hoeven geen toestemming te geven voor het delen van andere locatiegerelateerde gegevens. Wanneer de klant toestemming geeft voor het delen van zijn locatie,

¹² Dossierstuk 113 bij het onderzoeksrapport.

¹³ Dossierstuk 123 bij het onderzoeksrapport.

¹⁴ Dossierstuk 123 bij het onderzoeksrapport.

¹⁵ Dossierstukken 123 en 131 bij het onderzoeksrapport.

¹⁶ Dossierstuk 20 bij het onderzoeksrapport.

¹⁷ Dossierstukken 20 en 49 bij het onderzoeksrapport.

¹⁸ Yango Privacy Policy (19 maart 2025), https://yango.com/legal/yango_privacy_notice/en/19032025/.

Datum
1 april 2026

Ons kenmerk
2025-005323

kan de chauffeur de precieze locatie van klanten zien op de kaart op basis van GPS data, Wifi-netwerken of een combinatie van allebei. Klanten kunnen de locatie van de chauffeur ook live volgen.¹⁹

19. Ridetech kan via de Yango-app aan betrokkenen toegangsrechten vragen om:²⁰

- a) foto's en video's te maken, zodat de klant een foto of een scan kan maken van het nummer van de bankkaart met de telefooncamera in plaats van handmatig typen van dit nummer. De app slaat geen afbeeldingen op;
- b) GPS-gegevens en netwerkgebaseerde locatie-informatie te lezen, zodat de exacte ophaallocatie van de klant wordt bepaald. Deze informatie kan afkomstig zijn van GPS, bekende Wi-Fi-netwerken, of beide;
- c) toegang tot de microfoon te verkrijgen. In sommige landen kunnen klanten gebruikmaken van spraakherkenning om een bestemmingsadres op te geven of om berichten te sturen naar de chauffeur. Dit is ook mogelijk in Noorwegen;
- d) telefoonnummers direct te bellen, zodat de klant de chauffeur via de app met slechts één klik kan bellen;
- e) de status en identificerende informatie van de telefoon te lezen. Als de klant geen toegang geeft aan de app tot de identificerende informatie van de telefoon, gerelateerd aan Android device ID (IMEI), kan de klant geen kortingscodes gebruiken. Volgens het beleid zijn de promocodes van gebruikers gekoppeld aan hun apparaat-ID's ter voorkoming van fraude;
- f) gegevens in de USB-opslag te wijzigen, verwijderen of te lezen met als doel het kunnen opslaan van kaarten op de telefoon. Dit zou de Yango-app beter en sneller maken en mobiele data, opslag en batterij besparen. Als de klant geen toegangsrechten verleent voor deze functie, zal de app langzamer werken, aangezien de klant dan steeds moet wachten tot de kaarten geüpload zijn;
- g) synchronisatie-instellingen te lezen/synchronisatie in- en uitschakelen;
- h) netwerkverbindingen te bekijken en volledige toegang te krijgen tot het netwerk. Het geautoriseerde systeem controleert welke internetverbindingen beschikbaar zijn en kiest de meest geschikte internetverbinding.
- i) te voorkomen dat de telefoon in slaapstand gaat. Er kunnen meldingen gestuurd worden wanneer er een orderupdate is, bijvoorbeeld wanneer de chauffeur is gearriveerd op de ophaallocatie;
- j) Wi-Fi-verbindingen te bekijken en om verbinding te kunnen maken of verbreken met deze Wi-Fi verbindingen, zodat het vermogen van de app om de locatie van de klant te achterhalen, verbeterd kan worden;
- k) gegevens van het internet te ontvangen, voor de operabiliteit van de app. Deze functie kan niet worden uitgeschakeld;
- l) te trillen wanneer de telefooncamera het kaartnummer na het scannen met succes herkent;

¹⁹ Yango access to device, yango.com/legal/app-permissions_en/.

²⁰ Onderzoeksrapport, p 18 en 19).

Datum
1 april 2026

Ons kenmerk
2025-005323

- m) de *'install referrer API'* af te spelen. Hiermee kunnen ontwikkelaars niet-identificerende informatie ontvangen over de installatie van apps, zoals waar gebruikers deze vinden en wanneer ze deze installeren. Het is een middel om distributiekkanalen te monitoren en te beschermen tegen fraude;
- n) de app op de achtergrond te laten werken, zodat bepaalde informatie geüpdatet kan worden. Wanneer de app op de achtergrond werkt, maakt de app geen gebruik van de toegangsrechten tot de camera of microfoon.
20. Ridetech verwerkt voor de diensten zij aanbiedt via de Yango-app de volgende (categorieën) van persoonsgegevens van klanten:
- a. Telefoonnummer;
 - b. E-mailadres;
 - c. Elektronische identificatie data;
 - d. Datum en tijdstip van toegang tot en het gebruik van de diensten en/of de telefoonapp;
 - e. Informatie met betrekking tot activiteiten die plaatsvinden gedurende het gebruik van de diensten en/of de telefoonapp;
 - f. Chatgesprekken;
 - g. Telefoongesprekken;
 - h. Login informatie;
 - i. (Geo)locatie;
 - j. Details van de bestellingen;
 - k. Cookies (of soortgelijke technologieën);²¹
 - l. Details van de browser en/of telefoonapp;²²
 - m. Bankgegevens (zoals informatie over de betaalmethode).²³
21. Ridetech verwerkt voor de diensten die zij aanbiedt via de Yango-app de volgende (categorieën) van persoonsgegevens van chauffeurs:²⁴
- a. Naam;
 - b. Socialezekerheidsnummer;
 - c. Identificatienummer;
 - d. Geboortedatum;
 - e. Geboorteplaats;
 - f. Gender;
 - g. Nationaliteit;
 - h. Foto;
 - i. Telefoonnummer;

²¹ Dossierstuk 43 bij het onderzoeksrapport, p.11.

²² Dossierstuk 87 bij het onderzoeksrapport.

²³ Dossierstuk 87 bij het onderzoeksrapport, p. 31.

²⁴ Dossierstuk 43 bij het onderzoeksrapport, p.11.

Datum
1 april 2026

Ons kenmerk
2025-005323

- j. Officieel woonadres;
- k. Details van het rijbewijs: voor- en achternaam, vervaldatum, entiteit die het rijbewijs heeft uitgegeven, documentnummer, plaats waar het rijbewijs is uitgegeven, autocategorie of categorieën waarvoor het rijbewijs geldt, gescande kopieën van de genoemde documenten.
- l. Chatgesprekken;
- m. Telefoongesprekken;
- n. Bankgegevens.²⁵

2.4 Doorgifte naar Rusland

- 22. Yandex.Taxi LLC, gevestigd in Rusland, is de ontvanger van persoonsgegevens die naar Rusland worden doorgegeven. Yandex.Taxi LLC geeft deze persoonsgegevens in Rusland door aan (sub)verwerker Yandex LLC. Vóór 27 november 2023 werden persoonsgegevens van alle betrokkenen bewaard en verwerkt in datacenters in Rusland. De persoonsgegevens werden versleuteld bewaard in Rusland. De encryptiesleutels werden ook bewaard in Rusland.²⁶ Uit overgelegde documentatie blijkt dat Ridetech na 27 november 2023 persoonsgegevens van betrokkenen uit Finland en Noorwegen verwerkt in de Amazon Web Services (AWS) datacenters in Frankfurt.
- 23. Na pseudonimisering en versleuteling worden persoonsgegevens vanaf 27 november 2023 nog steeds doorgegeven naar Rusland waar ze bewaard en verwerkt worden op de servers van Yandex.Taxi LLC en Yandex LLC. Voor deze doorgifte van persoonsgegevens gebruikt Ridetech standaardbepalingen. Standaardbepalingen zijn modelcontracten die de Europese Commissie heeft goedgekeurd. Wanneer een verwerkingsverantwoordelijke standaardbepalingen gebruikt en de daarin opgenomen regels toepast bij de doorgifte van persoonsgegevens naar een derde land, dan wordt geacht dat de verwerkingsverantwoordelijke daarmee passende waarborgen heeft getroffen.
- 24. De standaardbepalingen van 21 september 2021²⁷ noemen (in annex II) de volgende aanvullende technische maatregelen:
 - a. Gebruik van strikte toegangsbeperking ter bescherming van bestelgegevens en (geo)locatie van betrokkenen. Alle gegevens zijn versleuteld.
 - b. Gebruik van sterke versleuteling vóór doorgifte naar Rusland: bijv. sleutellengte, bedrijfsmodus en type versleuteling kunnen als robuust worden beschouwd tegen cryptoanalyse door de overheid;
 - c. Correcte implementatie van het versleutelingsalgoritme en door naar behoren onderhouden software, zonder bekende kwetsbaarheden, waarvan de conformiteit met de specificatie van het gekozen algoritme is geverifieerd, bijvoorbeeld door certificering;

²⁵ Dossierstuk 87 bij het onderzoeksrapport, p. 31.

²⁶ Dossierstukken 19 en 73 bij het onderzoeksrapport.

²⁷ Dossierstuk 56 bij het onderzoeksrapport.

Datum
1 april 2026

Ons kenmerk
2025-005323

- d. Het op betrouwbare wijze beheren van de encryptiesleutels (gegenereerd, beheerd, opgeslagen en indien relevant, gekoppeld aan de identiteit van een beoogde ontvanger, en ingetrokken);
 - e. Het uitsluitend bewaren van de encryptiesleutels onder de controle van de gegevensexporteur of door een entiteit in de EER die door de exporteur wordt vertrouwd of binnen een jurisdictie die een beschermingsniveau biedt dat in wezen gelijkwaardig is aan het niveau dat binnen de EER wordt gewaarborgd.
25. De standaardbepalingen van 21 september 2021 noemen (in annex II) de volgende aanvullende organisatorische maatregelen:
- a. Markering en segregatie van de EER/EU-gegevens in de informatiesystemen wordt geïmplementeerd bij de controle van de toegang tot gegevens over ritten die in verschillende gebieden in het 'admin panel' zijn gemaakt;
 - b. Verbod op toegang tot deze gegevens door de Russische overheidsinstanties;
 - c. Implementatie van het goedkeuringsbeleid van de Functionaris Gegevensbescherming voor elke openbaarmaking/doorgifte van gegevens aan derden, met inbegrip van Russische overheidsinstanties;
 - d. Invoering van mechanismen voor het uitbannen van automatiseren voor pogingen van overheidsinstanties om toegang te krijgen tot EU-gegevens;
 - e. Vaststelling en publicatie van voorwaarden voor openbare verzoeken (officieel, gemotiveerd, enz.);
 - f. Regelmatige uitvoering van informatiebeveiligingsaudits door de gegevensexporteur;
 - g. Implementatie van beleid voor informatiebeveiliging, 'Bring Your Own Device', toegang op afstand, wachtwoorden, het delen van gegevens op verzoek van autoriteiten en ander strikt gegevensbeveiligings- en privacybeleid binnen de importerende dochteronderneming. Het beleid moet gebaseerd zijn op EU-certificering of gedragscodes of internationale normen (bijvoorbeeld ISO-normen) en 'best practices' (bijvoorbeeld ENISA:: Europese agentschap voor cyberbeveiliging), rekening houdend met de stand van de techniek, afhankelijk van het risico van de categorieën verwerkte gegevens;
 - h. Vaststellen van het proces van uitvoering van de instructies van de gegevensexporteur omtrent de rechten van betrokkenen en het wissen van gegevens (wie en hoe, aanvaarden, evalueren, registreren van instructies, wie gaat de instructies uitvoeren en op welke manier, en de status melden aan de Functionaris Gegevensbescherming (hierna: FG) van de exporteur);
 - i. Vaststelling van een adequaat intern proces met duidelijke toewijzing van verantwoordelijkheden voor gegevensdoorgiften, meldingskanalen en standaardwerkprocedures in geval van formele of informele verzoeken van overheidsinstanties;
 - j. Opleiden op het gebied van gegevensbescherming van al het personeel dat betrokken is bij de verwerking van EU-gegevens;
 - k. Het uitvoeren van 'refreshers';

Datum
1 april 2026

Ons kenmerk
2025-005323

- l. Ontwikkeling van specifieke opleidingsprocedures voor personeel dat belast is met het beheer van verzoeken om toegang tot persoonsgegevens afkomstig van overheidsinstanties. Dit moet periodiek worden bijgewerkt om rekening te houden met nieuwe ontwikkelingen op het gebied van wetgeving en jurisprudentie in het derde land en in de EER;
 - m. Documentatie en registratie van toegangsverzoeken die worden ontvangen van overheidsinstanties en de reactie op deze toegangsverzoeken, samen met de juridische redenering en de betrokken actoren (bijvoorbeeld of de exporteur in kennis is gesteld en zijn antwoord, de beoordeling van het team dat met de behandeling van dergelijke verzoeken is belast, enz.);
 - n. Regelmatige publicatie van transparantieverlagen of samenvattingen met betrekking tot verzoeken van de overheid om toegang tot gegevens en het soort antwoord dat gegeven wordt hierop, voor zover publicatie hiervan toegestaan is op grond van de lokale wetgeving;
 - o. Ontwikkeling van 'best practices' om de FG en de juridische en interne afdelingen op passende wijze en tijdig te betrekken en toegang te verlenen tot informatie over aangelegenheden die verband houden met internationale gegevensoverdrachten;
 - p. Vaststelling en regelmatige evaluatie van het interne beleid om de geschiktheid van de uitgevoerde aanvullende maatregelen te beoordelen. Zo nodig aanvullende of alternatieve oplossingen aanwijzen en uitvoeren, om ervoor te zorgen dat een niveau van bescherming van de doorgegeven persoonsgegevens wordt gehandhaafd dat in wezen gelijkwaardig is aan het niveau dat binnen de EER wordt gewaarborgd.
26. De standaardbepalingen noemen (in annex II) verder de volgende aanvullende juridische en contractuele maatregelen:
- a. De gegevensimporteur is contractueel verplicht de exporteur bij te staan bij zijn beoordeling van de toegang tot gegevens door overheidsinstanties;
 - b. Er zijn garanties waarbij de importeur verklaart dat (1) hij niet doelbewust 'backdoors' of soortgelijke programmeringen heeft gecreëerd die kunnen worden gebruikt om toegang te krijgen tot het systeem en/of de doorgegeven persoonsgegevens; (2) hij zijn bedrijfsprocessen niet doelbewust heeft gecreëerd of gewijzigd op een wijze die de toegang tot de doorgegeven persoonsgegevens of systemen vergemakkelijkt; en (3) het nationale recht of overheidsbeleid de importeur niet verplicht om 'backdoors' te creëren of te onderhouden of de toegang tot de doorgegeven persoonsgegevens of systemen te vergemakkelijken of dat de importeur in het bezit moet zijn van de versleutelingsleutel of de versleutelingsleutel moet overhandigen;
 - c. De bevoegdheid van de exporteur om het contract op korte termijn op te zeggen in die gevallen waarin de importeur niet het bestaan van een 'backdoor' of soortgelijke programmering of gemanipuleerde bedrijfsprocessen of een verplichting om een van deze uit te voeren aan het licht brengt of de exporteur niet onmiddellijk in kennis stelt zodra hij van hun bestaan op de hoogte is;

Datum
1 april 2026

Ons kenmerk
2025-005323

- d. Het vaststellen van specifieke en strikte termijnen en procedures voor de snelle opschorting van de doorgifte van gegevens en/of de beëindiging van het contract en de terugzending of verwijdering van de door de importeur ontvangen gegevens;
 - e. De gegevensimporteur moet alle juridische of beleidsontwikkelingen volgen die ertoe kunnen leiden dat hij zijn verplichtingen niet kan nakomen, en de gegevensexporteur onverwijld in kennis stellen van dergelijke wijzigingen en ontwikkelingen, en zo mogelijk, vóór de uitvoering ervan, zodat de gegevensexporteur de gegevens van de gegevensimporteur kan terugvorderen;
 - f. De importeur moet zich committeren aan het toetsen van de rechtmatigheid van elk bevel tot openbaarmaking van gegevens, met name of het binnen de aan de verzoekende overheidsinstantie verleende bevoegdheden valt, en het bevel aanvechten indien hij na een zorgvuldige beoordeling concludeert dat er volgens het recht van het ontvangende land redenen zijn om dit te doen.
27. Op 4 april 2024 heeft Ridetech de standaardbepalingen geüpdatet.²⁸ In aanvulling op de bovenstaande maatregelen heeft Ridetech nieuwe technische en organisatorische maatregelen getroffen.
28. Ridetech noemt in (in annex II van) de bijgewerkte standaardbepalingen van 4 april 2024 de volgende aanvullende technische maatregelen:
- a. Pseudonimisering (tokenisering: het vervangen van de platte tekst door een willekeurig gegenereerd pseudoniem (alleen in de EU) voordat het voor verwerking naar Rusland wordt verzonden. Profielgegevens van eindgebruikers en chauffeurs worden vervangen door tokens) die binnen de EU plaatsvindt voordat persoonsgegevens naar Rusland worden doorgegeven;
 - b. Obfuscatie van persoonsgegevens (van toepassing op geospatiale gegevens) - het wijzigen of verminderen van de nauwkeurigheid van gegevens en het aggregeren ervan, waardoor de locatie minder nauwkeurig wordt;
 - c. Maskering van persoonsgegevens - vervanging van het aanzienlijke deel van gegevens dat gegevens structureel vergelijkbaar maakt met originele gegevens, maar nutteloos is voor koppeling aan een betrokkene en niet waardevol is voor onbevoegd personeel;
 - d. Ontkoppelingsbeginsel (identificerende informatie wordt gescheiden van de rest van de gegevens om de kans te verminderen dat gegevens alsnog gekoppeld kunnen worden);
 - e. Versleuteling voorafgaand aan de doorgifte zonder toegang door de importeurs tot platte tekstgegevens, versleuteling van gegevens in transit zonder toegang door de importeurs tot platte tekstgegevens;
 - f. Versleuteling at rest van persoonsgegevens met behulp van moderne versleutelingsalgoritmen (AES 256);
 - g. Versleuteling van persoonsgegevens in transit (HTTPS, TLS (tot en met 1.3. versie)) om communicatiebeveiliging te waarborgen;

²⁸ Dossierstuk 87 bij het onderzoeksrapport.

Datum
1 april 2026

Ons kenmerk
2025-005323

- h. Opslag van encryptiesleutels binnen de EU;
- i. Toegangscontroles die door gegevensexporteur worden toegepast, met inbegrip van machtigingen om de toegang tot persoonsgegevens te weigeren, op te schorten of in te trekken, ook in de systemen van de importeur, en om de algemene configuraties van het toegangscontrolesysteem te beheren;
- j. Configuratiebeheer van de Yango-app, inclusief machtigingen om de functionaliteit van de applicatie in bepaalde landen of geografische gebieden en beschikbaarheid voor partners en integraties met andere applicaties en diensten, te bevestigen of op te schorten,;
- k. Voortdurende geautomatiseerde monitoring van de verwerkingsactiviteit, met inbegrip van logbestanden en systeemrapporten;
- l. Beveiligingsonderhoud;
- m. Maatregelen ter waarborging van de systeemconfiguratie, met inbegrip van de standaardconfiguratie;
- n. Het regelmatig testen, beoordelen en evalueren van de doeltreffendheid van technische en organisatorische maatregelen om de beveiliging van de verwerking te waarborgen, met inbegrip van regelmatige audits, het automatiseren van 24/7-audits, regelmatige pentesten, 'bug bounty'-programma;
- o. Maatregelen voor gebruikersidentificatie en -autorisatie, waaronder 2FA (OTP) – login en wachtwoord authenticatie, samen met een tweede factor zoals een sms-code, beleid inzake bedrijfsapparaten: toegang tot gegevens is alleen toegestaan via zakelijke apparaten, authenticatiecontrole op basis van het 802.1X-protocol, werken buiten kantoor alleen via VPN;
- p. Maatregelen om ervoor te zorgen dat de logging van gebeurtenissen, met inbegrip van acties van systeemgebruikers, wordt geregistreerd en opgeslagen voor auditdoeleinden en dat alle acties van gebruikers worden geregistreerd, interne auditautomatisering om de registratie van gebeurtenissen te analyseren om abnormale afwijkingen op te sporen, een speciaal uitgebreid auditsysteem om de acties van gebruikers met betrekking tot persoonsgegevens te controleren (deze audit omvat acties tussen microdiensten);
- q. Maatregelen voor interne IT- en IT-beveiligingsgovernance en -beheer, met inbegrip van een instrument voor eindpuntdetectie en -respons dat kwaadwillige activiteiten analyseert en detecteert, antivirusbescherming, back-ups, toegangscontrole op netwerkniveau, beheersbaar model voor toegangscontrole, operationeel beveiligingscentrum;
- r. Beheersbaar model voor toegangscontrole, waarmee de beheerder van een exporteur de regels voor locatietoegang kan configureren (goedkeuringsbeleid van de FG);
- s. Toegangscontrole op netwerkniveau;
- t. Logische segregatie van gegevens per land en product (merk) op programmaniveau om ervoor te zorgen dat alle gegevens worden opgeslagen in overeenstemming met de toepasselijke vereisten.

29. Ridetech noemt in (in annex II van) de bijgewerkte standaardbepalingen van 4 april 2024 de volgende aanvullende organisatorische maatregelen:

Datum
1 april 2026

Ons kenmerk
2025-005323

- a. Instructies en beleid;
- b. Bewustmakingsmechanismen en regelmatige opleidingen;
- c. Verplichtingen inzake gegevensbescherming zijn opgenomen in contracten met werknemers;
- d. Antecedentenonderzoeken voor werknemers;
- e. Fysieke beveiligingsmaatregelen, met inbegrip van maatregelen om ervoor te zorgen dat de beschikbaarheid van en de toegang tot gegevens tijdig worden hersteld in geval van een fysiek of technisch incident;
- f. Alle gegevens worden bewaard in de eigen datacenters van de importeurs die 24/7 onder fysieke controle staan;
- g. Beveiliging van bedrijfsruimten en fysieke toegangscontrole.

2.5 Russische wetgeving

30. De geldende Russische wetgeving is als volgt:

Criminal Procedure Code of the Russian Federation No.174-FZ of December 18, 2001
Code of Administrative Offences of the Russian Federation No. 195-FZ of December 30, 2001
Federal Law of the Russian Federation No. 149-FZ of July 27, 2006 on Information, Information Technologies and Protection of Information
Federal Law of the Russian Federation No. 152-FZ of July 27, 2006 on Personal Data
Decree of the Government of the Russian Federation No. 228 of March 16, 2009 on the Federal service for Supervision of Communications, Information Technology and Mass Media
Decree of the Government of the Russian Federation No. 743 of July 31, 2014 on the Rules of Cooperation of Organizers of Distribution of Information on the Internet
Federal Law of the Russian Federation No. 374-FZ and No. 376-FZ of July 6, 2016
Order of the Ministry of Digital Development and Communications No. 571 of October 29, 2018
Decree of the Government of the Russian Federation No. 1526 of September 23, 2020

Datum
1 april 2026

Ons kenmerk
2025-005323

Decree of the Government of the Russian Federation, No. 1101 of 4 July 2023
Federal Law of the Russian Federation No. 580-FZ of September 1, 2023 on the Organization of Passengers and Baggage Transportation by Passenger taxi in Russia
Order of the Government of the Russian Federation No. 256 of March 1, 2024
Federal Law of the Russian Federation No. 144-FZ of August 12, 1995 on Operational Search Activities

31. Het toezicht op de naleving van de privacywetgeving is in Rusland belegd bij de *Federal Service for Supervision of Communications, Information Technology, and Mass Media* (hierna: *Roskomnadzor*). *Roskomnadzor* is een uitvoerende instantie, die onderdeel uitmaakt van het Ministerie van Digitale Ontwikkeling, Communicatie en Massamedia van Rusland. De voorzitter van *Roskomnadzor* wordt aangesteld en ontslagen door de overheid van Rusland op advies van de minister van communicatie en massamedia.²⁹

Russische Taxiwet

32. De Russische Taxiwet is per 1 september 2023 in werking getreden. Deze wet verplicht taxivervoerders om een digitaal of analoog 'logboek' bij te houden.³⁰ Taxivervoerders moeten voor iedere taxirit de onderstaande gegevens invullen in een logboek:
- a. Het bestelnummer van de taxi;
 - b. Tijd en datum waarop de taxibestelling is geaccepteerd;
 - c. Datum waarop de taxibestelling is voltooid;
 - d. Het begin- en eindpunt van de taxirit;
 - e. Het merk, model en kenteken van het voertuig, en de achternaam, voornaam en patroniem (indien van toepassing) van de chauffeur;
 - f. De geplande en werkelijke aankomsttijd en de tijdsduur van de taxirit;
 - g. De methode waarmee de taxibestelling was geplaatst en het telefoonnummer van de klant die de bestelling heeft geplaatst;
 - h. Elke aanvullende eis die is gesteld door de klant die de bestelling heeft geplaatst, met inbegrip van de eis om elk kind van een kinderbeveiligingssysteem te voorzien of het vervoeren van een passagier die mindervalide is en diens rolstoel.

²⁹ Dossierstuk 86 bij het onderzoeksrapport.

³⁰ Artikel 11, zevende lid, en artikel 19, elfde lid, Russische Taxiwet.

Datum
1 april 2026

Ons kenmerk
2025-005323

33. De taxivervoerders zijn verplicht om de hierboven genoemde gegevens voor minstens zes maanden te bewaren na het voltooiën van de taxirit.³¹ Ook zijn taxivervoerders verplicht om gegevens te verschaffen, in de door de wet omschreven gevallen, wanneer een bevoegde instantie daarnaar vraagt. De bevoegde instantie is de federale uitvoerende instantie (of een regionaal kantoor daarvan) die verantwoordelijk is voor de veiligheid, of de federale uitvoerende instantie die verantwoordelijk is voor het ontwikkelen en implementeren van staatsbeleid en juridische regulering op het gebied van binnenlandse zaken of diens regionaal kantoor.
34. Taxivervoerders zijn ook verplicht om aan de federale uitvoerende instantie, verantwoordelijk voor de veiligheid, toegang te verschaffen tot informatiesystemen en databases die gebruikt worden voor het ontvangen, bewaren, verwerken en doorgeven van taxibestellingen op een wijze die voorgeschreven is door de Russische overheid.³²
35. In de *'Decree of the Government of the Russian Federation of 4 July 2023, No. 1101'* staan voorschriften die gelden voor de toegang door de Russische autoriteiten tot de informatiesystemen en databases van taxivervoerders. Hieruit volgt tevens dat taxivervoerders gebonden zijn aan een geheimhoudingsplicht ten aanzien van de interacties met de FSB (de Russische binnenlandse veiligheidsdienst).

SORM

36. De *'Federal Law of the Russian Federation No. 149-FZ of July 27, 2006'* (hierna: Information Act) bepaalt wat een *Internet Communications Organisers* (hierna: ICO) is.³³ Dat is een persoon of entiteit die zorgt voor de werking van informatiesystemen en/of programma's voor elektronische apparaten, met als doel het ontvangen, verzenden, leveren en/of verwerken van elektronische communicatie op het internet. Zowel Yandex.Taxi LLC als Yandex LLC zijn aangemerkt als een ICO. Zij staan ook als zodanig geregistreerd in het ICO-register. Daarmee is de Information Act op hen van toepassing.
37. Voor ICO's zijn in 2016 aanvullende verplichtingen geïntroduceerd in de *'Federal Law of the Russian Federation No. 374-FZ and 376-FZ of July 6, 2016'* (hierna samen: *'Yarovaya Law'*). Sindsdien zijn ICO's verplicht bepaalde informatie te verstrekken aan rechtshandavingsinstanties of veiligheidsdiensten.³⁴ Ook zijn ICO's verplicht om alle informatie te verstrekken die nodig is om versleutelde elektronische communicatie te decoderen.³⁵
38. Om genoemde informatie te kunnen verschaffen, moeten ICO's de vereiste apparatuur op hun softwaresystemen installeren. Deze apparatuur wordt aangemerkt als de *System for Operative Investigative Activities* (hierna: SORM). Alle organisaties, waaronder ICO's, zijn verplicht tot geheimhouding. Zij mogen geen informatie delen over de SORM of de technische details van de integratie van de SORM in hun

³¹ Artikel 11, achtste lid, Russische Taxiwet.

³² Artikel 14, zevende lid, Russische Taxiwet.

³³ Artikel 10.1, eerste lid, Information Act.

³⁴ Artikel 10.1, derde lid, Information Act.

³⁵ Artikel 10.1, vierde lid, Information Act.

Datum
1 april 2026

Ons kenmerk
2025-005323

systemen.³⁶ Het delen van deze informatie wordt gestraft met een maximale administratieve boete tot 6 miljoen Russische Roebels.³⁷

39. In het onderzoeksrapport is geconcludeerd dat Ridetech en Yandex.Taxi LLC gezamenlijke verwerkingsverantwoordelijke zijn voor de onderzochte gegevensverwerking.³⁸ Daarnaast is in het onderzoeksrapport geconcludeerd dat Ridetech niet heeft kunnen aantonen dat de doorgifte van persoonsgegevens aan Yandex.Taxi LLC en Yandex LLC voldoet aan hoofdstuk V van de AVG. Ridetech heeft onvoldoende aangetoond dat zij met de door haar genomen maatregelen, die bestaat uit het gebruik maken van standaardbepalingen, in het kader van de doorgifte naar Rusland een beschermingsniveau waarborgt dat in elk geval gelijkwaardig is aan het beschermingsniveau binnen de Europese Unie.

3. Juridisch kader

40. Het relevante juridisch kader is in bijlage 1 opgenomen en maakt onderdeel uit van dit besluit.

4. Zienswijze Ridetech

41. Ridetech heeft –samengevat – de volgende zienswijze op het onderzoeksrapport gegeven.
42. Volgens Ridetech is er geen sprake van gezamenlijke verwerkingsverantwoordelijkheid tussen Ridetech en Yandex.Taxi LLC. Daarnaast vindt Ridetech dat er geen sprake is van ongeoorloofde doorgifte van persoonsgegevens.

Verwerkingsverantwoordelijkheid

43. Volgens Ridetech wordt in het onderzoeksrapport ten onrechte geconcludeerd dat Ridetech en Yandex.Taxi LLC gezamenlijke verwerkingsverantwoordelijke zijn. Yandex.Taxi LLC verwerkt geen persoonsgegevens voor haar eigen doeleinden. Yandex.Taxi LLC is slechts een softwareleverancier die een Software as a Service-oplossing (hierna: SaaS-oplossing) aanbiedt. Ridetech heeft met Yandex.Taxi LLC een licentieovereenkomst gesloten voor het afnemen van de SaaS-oplossing. Deze licentieovereenkomst bevat standaardbepalingen. Eén daarvan is dat Ridetech zonder toestemming van Yandex.Taxi LLC de software niet mag wijzigen.
44. Ridetech vindt dat de AP in het onderzoeksrapport het karakter en de eigenschappen van een SaaS-oplossing miskent. De afnemer van een SaaS-oplossing heeft beperkte zeggenschap over de software zelf, omdat de softwareleverancier verantwoordelijk is voor het onderhoud en beheer ervan. De SaaS-oplossing van Yandex.Taxi LLC is een op zichzelf staande dienst die Ridetech afneemt en verder aankleedt met het

³⁶ Artikel 10.1, vierde lid, Operational Search Activities Act (hierna: OSAA).

³⁷ Artikel 13.31, Code of Administrative Offences of the Russian Federation.

³⁸ Onderzoeksrapport, pagina 35.

Datum
1 april 2026

Ons kenmerk
2025-005323

doel om haar diensten via de Yango-app aan te bieden. Ridetech stelt dat zij de Yango-app ook zou kunnen aanbieden indien een andere softwareontwikkelaar de SaaS-oplossing hiervoor zou leveren.

Passende waarborgen

45. Ridetech benadrukt dat zij privacy hoog in het vaandel heeft staan. Zij heeft vanaf het eerste moment volledig meegewerkt met de toezichthouders over de verwerking van persoonsgegevens. Ridetech heeft vragen altijd direct en volledig beantwoord en haar systemen en/of werkwijze op verzoek van toezichthouders aangepast.
46. De maatregelen die Ridetech tot op heden heeft genomen, zijn verbeteringen ten opzichte van de situatie in mei 2022 en die in het najaar van 2023. Er vinden nu regelmatig audits plaats binnen de Ridetech Group. Deze audits worden uitgevoerd door het Security Team in Servië. Ook is Ridetech sinds januari 2025 bezig met het aanpassen van de werkwijze waarmee gegevens aan Yandex.Taxi LLC worden verstrekt. Sinds 11 juli 2025 lopen alle datastromen volledig via dataservers in de EU en dus ook de datastromen waarin geen persoonsgegevens worden verwerkt. Dit betekent dat Ridetech alleen maar versleutelde gegevens aan Yandex.Taxi LLC in Rusland kan verstrekken.
47. Ridetech betoogt verder dat er voldoende technische, organisatorische en contractuele maatregelen zijn genomen. Anders dan in het onderzoeksrapport wordt geconcludeerd, voldoet Ridetech wel aan de vereisten die gelden voor internationale doorgifte van persoonsgegevens. Ten eerste omdat Ridetech deze gegevens heeft gepseudonimiseerd. Ten tweede omdat Ridetech deze gegevens heeft versleuteld. De sleutels of koppelingcodes die nodig zijn om de geaggregeerde en versleutelde gegevens tot natuurlijke personen te kunnen herleiden, bevinden zich in het datacenter in de EU. Ridetech stelt dat met de getroffen technische maatregelen het voor Yandex.Taxi LLC en Yandex LLC niet mogelijk is om de geïmporteerde gegevens te herleiden tot natuurlijke personen. Daarom zijn deze gegevens als zodanig geen persoonsgegevens.
48. Voor zover de Russische autoriteiten al een vordering zouden doen om toegang te krijgen tot gegevens van betrokkenen uit de EU, beschikken Yandex.Taxi LLC en Yandex LLC niet over de mogelijkheid om aan een dergelijke vordering te voldoen. Zelfs in het meest vergaande scenario waarbij Russische autoriteiten toegang zouden verkrijgen tot de versleutelde en gepseudonimiseerde gegevens, zouden deze gegevens van geen enkel nut zijn, omdat de Russische autoriteiten via Yandex.Taxi LLC of Yandex LLC niet aan de onderliggende, oorspronkelijke gegevens kunnen komen.

Risicogebaseerde aanpak

49. Ridetech wijst er verder op dat het recht op bescherming van persoonsgegevens, neergelegd in artikel 8 Handvest, niet absoluut is. Dit recht moet worden afgewogen tegen andere fundamentele rechten en vrijheden, zoals het recht van vrijheid van ondernemerschap. Ridetech heeft voor de doorgifte van gegevens naar Rusland een op risico gebaseerde aanpak gehanteerd. Zij heeft een Transfer Impact Assessments (hierna: TIA) opgesteld en daarmee risico's aan de doorgifte van de gegevens naar Rusland

Datum
1 april 2026

Ons kenmerk
2025-005323

beoordeeld. Volgens Ridetech focust de AP in het onderzoeksrapport ten onrechte op de theoretische mogelijkheid van toegang door de Russische autoriteiten in de gegevens die via doorgifte in Rusland worden verwerkt.

Russisch recht

50. Volgens Ridetech valt zij niet onder de reikwijdte van de Russische wetgeving. Yandex.Taxi LLC en Yandex LLC vallen daarentegen wel onder de Russische Information Act. Zij worden namelijk aangemerkt als een ICO en staan ook geregistreerd met bepaalde diensten in het Russische ICO-register. Volgens Ridetech is het echter onjuist dat Yandex.Taxi LLC en Yandex LLC op grond van de Information Act algemene en directe toegang tot de informatiesystemen moeten verlenen aan de Russische autoriteiten. Ook is in het onderzoeksrapport onvoldoende bewijs geleverd voor de conclusie dat de Russische autoriteiten wel algemene en directe toegang hebben tot de geïmporteerde gegevens.
51. Volgens Ridetech zijn Yandex.Taxi LLC en Yandex LLC op grond van de Information Act verplicht om de SORM te implementeren. SORM kent verschillende varianten en de variant voor Yandex.Taxi LLC en Yandex LLC wordt 'HSS ICO' genoemd. HSS ICO is een verzamelterm voor de software en hardware die ICO's in hun interne infrastructuur moeten implementeren. Via HSS ICO kunnen Russische autoriteiten gegevens opvragen bij ICO's en kunnen ICO's vervolgens zelf selecteren welke informatie zij via dit systeem met de Russische autoriteiten delen. Op basis van Russische regelgeving (Order No. 571) zijn er vier kanalen waarmee informatie met binnen HSS ICO kan worden uitgewisseld:
- Kanaal 1: het controle kanaal;
 - Kanaal 2: het datakanaal;
 - Kanaal 3: het configuratiekanaal;
 - Kanaal 4: het ongestructureerde kanaal.
52. ICO's zijn op basis van Russische regelgeving niet verplicht om verdere medewerking te verlenen dan de bovenstaande beschrijving van HSS ICO. Yandex.Taxi LLC en Yandex LLC zijn wel ICO's, maar zij vallen echter niet onder het regime dat geldt voor telecomaانبieders. Volgens Ridetech is in het onderzoeksrapport daarom ook ten onrechte verwezen naar uitspraken van het EHRM (zaak Zakharov³⁹ en zaak Podchasov⁴⁰) waarin het draaide om het verstrekken van gegevens door telecomaانبieders. Alleen telecomaانبieders hebben op grond van de Information Act en 'Order No. 268' de plicht om de mogelijkheid tot tappen aan te bieden. Deze verplichting geldt dan ook niet voor Yandex.Taxi LLC en Yandex LLC.

³⁹ EHRM 4 december 2015, [ECLI:CE:ECHR:2015:1204JUD004714306](#) (*Zakharov v. Russia*).

⁴⁰ EHRM 13 februari 2024, [ECLI:CE:ECHR:2024:0213JUD003369619](#) (*Podchasov v. Russia*).

Datum
1 april 2026

Ons kenmerk
2025-005323

53. Tot slot heeft Ridetech de AP geïnformeerd dat alle servers van de 'Yango Group' in 2025 naar Servië zijn verplaatst. In dit verband heeft Ridetech een nieuwsartikel overgelegd ter onderbouwing van de informatie.⁴¹

5. Beoordeling

5.1 Bevoegdheid AP

54. Ridetech is in Nederland gevestigd en biedt haar diensten aan via de Yango-app in Noorwegen en Finland. De diensten van Ridetech in Noorwegen en Finland zijn per 1 maart 2025 ondergebracht bij twee nieuw opgerichte dochterondernemingen in respectievelijk Noorwegen en Finland.⁴² In dit geval verwerkt Ridetech persoonsgegevens in meer dan één lidstaat. Ridetech heeft haar hoofdvestiging (en tot 1 maart 2025 de enige vestiging in de EER) in Nederland. Dit betekent dat er sprake is van een grensoverschrijdende verwerking en dat (dus) de AP als leidende toezichhouder bevoegd is om tegen deze verwerking op te treden.⁴³

5.2 Verwerking van persoonsgegevens

55. Ridetech verwerkt persoonsgegevens van betrokkenen via de Yango-app voor haar dienstverlening. Hiervoor is in paragraaf 2.3 weergegeven welke persoonsgegevens Ridetech voor haar dienstverlening verwerkt. Daarnaast deelt Ridetech persoonsgegevens met de Russische ontvangers, Yandex.Taxi LLC en Yandex LLC. Het doorgeven van persoonsgegevens aan een andere entiteit kwalificeert eveneens als een verwerking in de zin van artikel 4, aanhef en onder 2, AVG.

5.3 Verwerkingsverantwoordelijke

56. In het onderzoeksrapport zijn Ridetech en Yandex.Taxi LLC gezamenlijk als verwerkingsverantwoordelijke aangemerkt voor de verwerking van persoonsgegevens van betrokkenen via de Yango-app. Ridetech stelt zich op het standpunt dat alleen zij als verwerkingsverantwoordelijke moet worden aangemerkt en dat Yandex.Taxi LLC slechts verwerker is van de persoonsgegevens van betrokkenen die de Yango-app gebruiken.
57. Het Hof van Justitie van de Europese Unie (hierna: HvJ EU) heeft bepaald dat de betrokkenheid bij de vaststelling van het doel van en de middelen voor de verwerking verschillende vormen kan aannemen en het resultaat kan zijn van zowel een gezamenlijk besluit van twee of meer entiteiten als het resultaat van convergerende besluiten van die entiteiten.⁴⁴ Wanneer het gaat om convergerende besluiten, dan moeten

⁴¹ Bijlage 4 bij dit besluit: UAE-based De Yango-app Group to open flagship data centre hub in Serbia to boost its global infrastructure' van 12 juni 2025.

⁴² Dossierstuk 123 bij het onderzoeksrapport.

⁴³ Artikel 56, eerste lid, AVG.

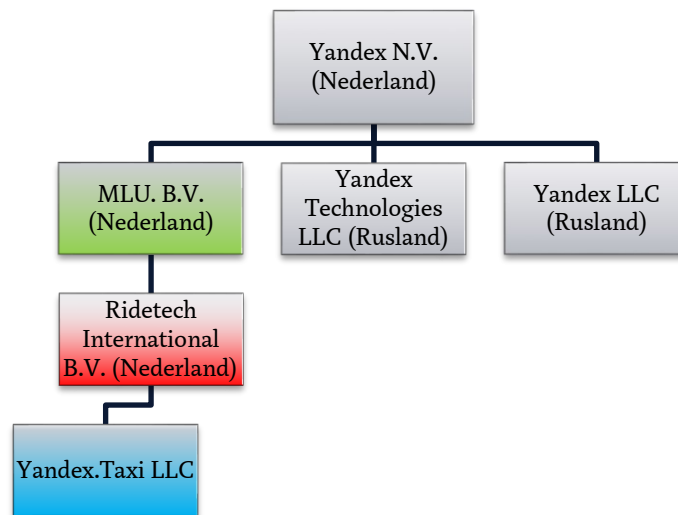
⁴⁴ HvJ EU 7 maart 2024, [ECLI:EU:C:2024:214](#) (*IAB Europe*), ro. 59.

Datum
1 april 2026

Ons kenmerk
2025-005323

die besluiten elkaar aanvullen zodat elk ervan een concreet effect heeft op de vaststelling van het doel en de middelen voor de verwerking.⁴⁵

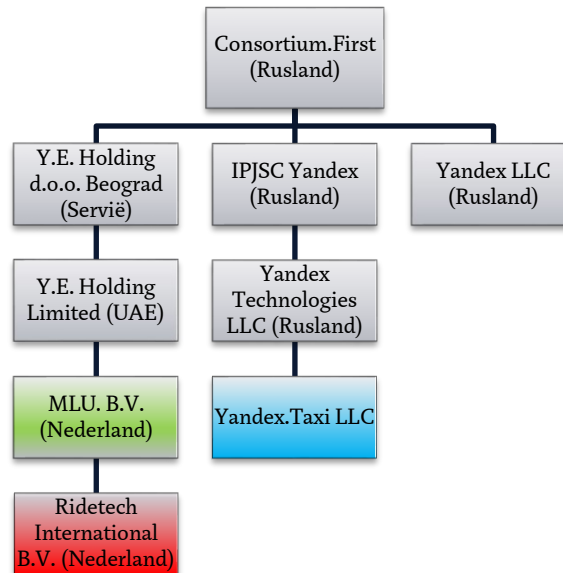
58. Vaststaat dat Ridetech tot februari 2024 onderdeel uitmaakte van een concern met een zeer omvangrijke organisatiestructuur en dat Yandex.Taxi LLC in ieder geval tot februari 2024 een dochteronderneming van Ridetech was.⁴⁶
59. In de periode tussen februari en juli 2024 is het concern geherstructureerd en daarmee is Yandex.Taxi LLC een dochteronderneming van de Russische Yandex Technologies LLC geworden.
60. Schematisch ziet de – versimpelde – organisatiestructuur vóór juli 2024 er als volgt uit:



61. Na juli 2024 is Yandex N.V. overgenomen door Consortium.First. Schematisch ziet de – versimpelde – organisatiestructuur er als volgt uit:

⁴⁵ HvJ EU 7 maart 2024, [ECLI:EU:C:2024:214](#) (*IAB Europe*), ro. 59.

⁴⁶ Dossierstukken 29, 35 en 110 bij het onderzoeksrapport.



62. Uit het voorgaande volgt dat Ridetech en Yandex.Taxi LLC weliswaar juridisch gezien afzonderlijke entiteiten zijn, maar dat zij niettemin tot hetzelfde concern behoren. De Yango-app is gebouwd met de software waarop de intellectuele eigendomsrechten van Yandex.Taxi LLC rusten. Deze software (de zogenoemde SaaS-oplossing) wordt door Yandex.Taxi LLC, bij wijze van dienst, aangeboden aan haar zusterondernemingen, waaronder dus ook Ridetech. De voornoemde software is essentieel voor de ride-hailing diensten die binnen het concern door Ridetech en haar zusterondernemingen worden verleend. Als ontwikkelaar en leverancier van deze software bepaalt Yandex.Taxi LLC hoe de Yango-app eruitziet en welke persoonsgegevens verwerkt moeten worden via deze app. Ook mogen anderen dan Yandex.Taxi LLC geen wijzigingen aanbrengen in de software..⁴⁷
63. Tegelijkertijd heeft Ridetech de taak om de Yango-app in Noorwegen en Finland uit te baten en voor dat doel heeft Ridetech verschillende overeenkomsten gesloten met bijvoorbeeld AWS, voor dataopslag, of met DPO Europe GmbH, voor de inhuur van een FG. De omstandigheid dat Ridetech met gebruikers van de Yango-app een overeenkomst sluit en als contactpunt optreedt bij onder meer inzageverzoeken van gebruikers of datalekken meldt bij de AP, zijn in dit kader handelingen van bijkomende aard. Feitelijk is de situatie zo dat de Yango-app in Noorwegen en Finland als dienst op de markt is gebracht en dat twee entiteiten, behorend tot hetzelfde concern, middelen inzetten met het doel om de Yango-app als dienst beschikbaar te stellen en te houden voor gebruikers in Noorwegen en Finland.
64. Gelet op het vorenstaande is de AP van oordeel dat Ridetech en Yandex.Taxi LLC samen het doel en de middelen bepalen voor verwerkingen van persoonsgegevens via de Yango-app en daarmee, als entiteiten die tot hetzelfde concern behoren, gezamenlijk verwerkingsverantwoordelijke zijn voor deze verwerkingen.

⁴⁷ Dossierstuk 45 bij het onderzoeksrapport, p. 4.

Datum
1 april 2026

Ons kenmerk
2025-005323

5.4 Internationale doorgifte van persoonsgegevens

65. Doorgifte van persoonsgegevens naar een derde land of aan een internationale organisatie kan plaatsvinden wanneer de Europese Commissie een zogenoemde adequaatheidsbesluit heeft genomen voor het betreffende land of de betreffende internationale organisatie.⁴⁸
66. De Europese Commissie heeft voor Rusland geen adequaatheidsbesluit vastgesteld. Het staat ook niet ter discussie dat Rusland geen passend beschermingsniveau waarborgt dat in grote lijnen overeenkomt met het beschermingsniveau dat in de EU/EER wordt geboden.
67. Bij afwezigheid van een adequaatheidsbesluit kan doorgifte niettemin plaatsvinden indien passende waarborgen worden geboden en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken.⁴⁹ Passende waarborgen kunnen worden geboden door, onder meer, standaardbepalingen (de zogenaamde SCC's) die door de Europese Commissie zijn vastgesteld.⁵⁰ In dit geval heeft Ridetech voor de doorgifte van persoonsgegevens naar Rusland gebruik gemaakt van dergelijke standaardbepalingen. Daarom moet de AP beoordelen of dit instrument passende waarborgen biedt voor de bescherming van persoonsgegevens.
68. Ridetech heeft gebruik gemaakt van standaardbepalingen⁵¹ die gelden voor doorgifte van persoonsgegevens tussen een verwerkingsverantwoordelijke en een verwerker. De AP heeft hiervoor, in randnummer 64, echter geconcludeerd dat Ridetech en Yandex.Taxi LLC gezamenlijk verwerkingsverantwoordelijken zijn. Daarom had Ridetech gebruik moeten maken van standaardbepalingen die gelden voor de doorgifte van persoonsgegevens tussen twee verwerkingsverantwoordelijken. Dat betekent dat Ridetech, door gebruik te maken van standaardbepalingen die gelden voor de doorgifte van persoonsgegevens tussen een verwerkingsverantwoordelijke en een verwerker, dus niet de juiste standaardbepalingen heeft gebruikt om passende waarborgen te treffen voor de doorgifte van persoonsgegevens van gebruikers van de Yango-app aan ontvangers in Rusland.⁵² Ondanks die omstandigheid, zal de AP hierna toch nog beoordelen of Ridetech passende waarborgen heeft getroffen voor genoemde doorgifte van persoonsgegevens.

5.4.1 Passende waarborgen

69. Zoals in paragraaf 2.4 van dit besluit is weergegeven, maakt Ridetech gebruik van standaardbepalingen. Om te beoordelen of Ridetech met haar standaardbepalingen passende waarborgen heeft geboden voor de doorgifte van persoonsgegevens van Finse en Noorse betrokkenen naar Rusland, maakt de AP onderscheid

⁴⁸ Artikel 45, eerste lid, AVG.

⁴⁹ Artikel 46, eerste lid, AVG.

⁵⁰ Artikel 46, tweede lid, onder c, AVG.

⁵¹ Dossierstukken 6, 79 en 87 bij het onderzoeksrapport.

⁵² De standaardbepalingen bevatten algemene bepalingen en drie verschillende modules: 1) doorgifte tussen twee verwerkingsverantwoordelijken, 2) doorgifte tussen verwerkingsverantwoordelijke en verwerker en 3) doorgifte tussen twee verwerkers. De verwerkingsverantwoordelijke(n) en verwerker(s) moeten de module kiezen die op hun situatie van toepassing is.

Datum
1 april 2026

Ons kenmerk
2025-005323

tussen enerzijds de periode (tot 27 november 2023) waarin de encryptiesleutels werden bewaard in datacenters in Rusland en anderzijds de periode (na 27 november 2023) waarin deze encryptiesleutels werden bewaard in datacenters in Frankfurt.

70. De AP stelt vast dat Ridetech in ieder geval tot 27 november 2023 persoonsgegevens heeft doorgegeven naar Rusland zonder dat zij daarbij passende waarborgen heeft getroffen. In de randnummers 22 en 23 van dit besluit is weergegeven dat Ridetech weliswaar tot 27 november 2023 persoonsgegevens alleen in versleutelde vorm op de servers in Rusland verwerkte, maar dat de encryptiesleutels waarmee deze persoonsgegevens weer 'ontsleuteld' konden worden, óók werden bewaard op dezelfde servers - in Rusland.
71. Gebleken is dat persoonsgegevens die Ridetech via de Yango-app verwerkte, eerst in de datacenters van AWS in Frankfurt werden opgeslagen. Na de opslag bij AWS stuurde Ridetech deze persoonsgegevens door naar de 'backend' server in Rusland. De 'backend' server verving de persoonsgegevens door gepseudonimiseerde 'identifiers' die vervolgens werden versleuteld op de 'personal' server. De bijbehorende encryptiesleutels werden in de RAM (het werkgeheugen) van diezelfde server bewaard. Dit betekent dat de persoonsgegevens in de 'personal' server óók weer konden worden ontsleuteld met de encryptiesleutels die op deze server werden bewaard.⁵³
72. De AP merkt op dit punt nog op dat Ridetech volgens haar standaardbepalingen (van 21 september 2021) encryptiesleutels alleen mag bewaren binnen de EER of in een land met een gelijkwaardig beschermingsniveau. Dit was dus niet het geval. De encryptiesleutels werden immers in Rusland bewaard, onder de controle van het plaatselijke 'Security Team'. Ridetech handelde dus zelfs in strijd met haar eigen standaardbepalingen.
73. Overigens heeft Ridetech niet inzichtelijk gemaakt op welke (andere) wijze haar standaardbepalingen van 21 september 2021 het risico op toegang door de Russische autoriteiten hebben kunnen voorkomen gedurende de periode waarin de encryptiesleutels samen met de versleutelde persoonsgegevens bewaard werden in Rusland.
74. Nu Ridetech in ieder geval tot 27 november 2023 de encryptiesleutels op dezelfde servers in Rusland bewaarde als de versleutelde persoonsgegevens van Finse en Noorse gebruikers van de Yango-app, heeft zij naar het oordeel van de AP geen passende waarborgen getroffen voor de doorgifte van persoonsgegevens.
75. In de periode na 27 november 2023 heeft Ridetech de werkwijze van doorgifte van persoonsgegevens naar Rusland gewijzigd. Deze wijziging houdt in dat persoonsgegevens van Finse en Noorse gebruikers van de Yango-app werden versleuteld en daarna werden opgeslagen op de servers van AWS in Frankfurt ('data at rest'). De encryptiesleutels van de versleutelde persoonsgegevens werden ook op de servers van AWS in Frankfurt opgeslagen. De versleutelde persoonsgegevens werden vervolgens naar Yandex.Taxi LLC en Yandex LLC in Rusland doorgegeven ('data in transfer').

⁵³ Dossierstuk 19 bij het onderzoeksrapport.

Datum
1 april 2026

Ons kenmerk
2025-005323

76. De AP moet dan ook beoordelen of Yandex.Taxi LLC en Yandex LLC als ontvangers van persoonsgegevens van Finse en Noorse gebruikers van de Yango-app over middelen beschikken waarvan redelijkerwijs te verwachten is dat zij die kunnen gebruiken om de Noorse en Finse gebruikers te identificeren.
77. De AP is van oordeel dat Yandex.Taxi LLC en Yandex LLC over deze middelen beschikken en licht dat als volgt toe.
78. Ridetech werd in de periode van 15 september 2020⁵⁴ tot 31 mei 2024⁵⁵ door één bestuurder bestuurd, de heer [VERTROUWELIJK].⁵⁶ Ook is hij in de periode van 1 mei 2020⁵⁷ tot 31 mei 2024⁵⁸ bestuurder van MLU B.V., de moederonderneming van Ridetech.⁵⁹ Vanaf 27 september 2022 is de heer [VERTROUWELIJK], samen met de heer [VERTROUWELIJK], bestuurder van MLU B.V.⁶⁰ Vaststaat dat de heer [VERTROUWELIJK] in ieder geval op 27 augustus 2024 nog bestuurder was van MLU B.V.⁶¹ Daarnaast is de heer [VERTROUWELIJK] ook bestuurder van de Russische Yandex.Taxi LLC. Dit volgt uit de standaardbepalingen van 21 september 2021⁶² en 4 april 2024,⁶³ die de heer [VERTROUWELIJK] als directeur van Yandex.Taxi LLC heeft ondertekend.
79. Uit voorgaande randnummer volgt dat zowel de ontvanger van persoonsgegevens (Yandex.Taxi LLC) als de exporteur van die persoonsgegevens (MLU B.V.) bestuurd werden door dezelfde persoon, de heer [VERTROUWELIJK]. De AP ziet in deze omstandigheid ruim voldoende grond voor de conclusie dat redelijkerwijs te verwachten is dat Yandex.Taxi LLC kan worden ingezet om Finse en Noorse gebruikers te identificeren. De bestuurder van een onderneming heeft immers alle bevoegdheden en toegang tot gegevens binnen de onderneming(en) die hij bestuurt. Dit illustreert de nauwe verwevenheid tussen Ridetech en Yandex.Taxi LLC, als entiteiten binnen het concern. De AP trekt daaruit de conclusie dat het identificeren van de Finse en Noorse gebruikers niet veel kosten, tijd of mankracht zou vergen van Yandex.Taxi LLC. Dat de persoonsgegevens van de Finse en Noorse gebruikers in de periode na 27 november 2023 gepseudonimiseerd en ('in transit' en 'at rest') versleuteld zijn en dat de encryptiesleutels niet meer worden bewaard in Rusland, laat onverlet dat de mogelijkheid bestaat dat de genoemde persoonsgegevens via de bestuurder van Yandex.Taxi LLC in Rusland alsnog ontsleuteld kunnen worden.⁶⁴ Dit betekent dat de versleutelde gegevens voor Yandex.Taxi LLC niet louter geanonimiseerde gegevens zijn, maar juist persoonsgegevens. De AP betreft hierbij ook de omstandigheid dat Ridetech en Yandex.Taxi LLC tot het zelfde concern behoren en zij hiërarchisch ondergeschikt zijn aan de wensen van het bestuur van hun moederonderneming ongeacht of beide ondernemingen dezelfde persoon als

⁵⁴ Dossierstuk 21 bij het onderzoeksrapport.

⁵⁵ Dossierstuk 107 bij het onderzoeksrapport.

⁵⁶ Dossierstuk 21 bij het onderzoeksrapport.

⁵⁷ Dossierstuk 11 bij het onderzoeksrapport.

⁵⁸ Dossierstuk 117 bij het onderzoeksrapport.

⁵⁹ Dossierstuk 11 bij het onderzoeksrapport.

⁶⁰ Dossierstuk 11 bij het onderzoeksrapport.

⁶¹ Dossierstuk 117 bij het onderzoeksrapport.

⁶² Dossierstuk 42 bij het onderzoeksrapport.

⁶³ Dossierstuk 87 bij het onderzoeksrapport.

⁶⁴ Vergelijk in dit kader HvJ EU 4 september 2025, [ECLI:EU:C:2025:645](#) (GAR/EDPS), r.o 68-90.

Datum
1 april 2026

Ons kenmerk
2025-005323

bestuurder hebben. De AP is dan ook van oordeel dat Yandex.Taxi LLC en Yandex LLC toegang kunnen krijgen tot persoonsgegevens van Finse en Noorse gebruikers van de Yango-app die op de 'backend' server in Rusland worden bewaard. Onder deze omstandigheden concludeert de AP dat Ridetech geen passende waarborgen heeft getroffen voor de doorgifte van persoonsgegevens.

5.4.2 Reikwijdte van de Russische wetgeving

80. Ook zal de AP beoordelen of de waarborgen die Ridetech meent te hebben genomen, gelet op de Russische regelgeving, passend zijn.
81. In randnummer 36 is weergegeven dat Yandex.Taxi LLC en Yandex LLC op grond van de Russische Information Act als ICO's worden aangemerkt. Uit de Information Act en de zogenoemde 'Yarovaya Law' volgt weliswaar niet dat alle ICO's algemene en directe toegang tot hun gegevens aan de autoriteiten moeten geven, maar bepaalde ICO's zijn wel verplicht om via de zogenoemde SORM informatie door te geven aan de autoriteiten. Het gaat dan om gegevens van:
- a) Geregistreerde gebruikers met IP-adressen waarvan de ICO vaststelt dat deze worden gebruikt binnen het Russische grondgebied;
 - b) Geautoriseerde gebruikers met IP-adressen waarvan de ICO vaststelt dat deze worden gebruikt binnen het Russische grondgebied;
 - c) Gebruikers die, gedurende registratie of tijdens het gebruik van de functionaliteiten van de ICO, een Russisch identiteitsdocument hebben overgelegd;
 - d) Gebruikers die voor de toegang tot de ICO gebruik maken van apparaten en/of programma's welke locatiegegevens doorsturen naar de ICO, wanneer de locatiegegevens aangeven dat de gebruiker zich (tijdelijk) binnen Russisch grondgebied bevindt;
 - e) Gebruikers die, gedurende registratie of tijdens het gebruik van de functionaliteiten van de ICO, als contactgegevens een telefoonnummer doorgeven welke is toegewezen door een Russische telecom aanbieder;
 - f) Gebruikers van wie de ICO door de relevante Russische autoriteiten is geïnformeerd dat deze zich bevinden op Russisch grondgebied.
82. Voornoemde gegevens zijn hoofdzakelijk van gebruikers die zich binnen het grondgebied van Rusland bevinden, maar het is niet uitgesloten dat een gebruiker van de Yango-app uit Finland of Noorwegen (tijdelijk) in Rusland heeft verbleven of over een telefoonnummer beschikt dat door een Russische telecomaandbieder is verstrekt. Wanneer één van deze situaties zich voordoet, dan kunnen de persoonsgegevens van betreffende gebruikers uit Finland en Noorwegen van de Yango-app door de Russische autoriteiten worden opgevraagd.
83. De AP heeft kennis genomen van het standpunt van Ridetech dat Yandex.Taxi LLC en Yandex LLC, als ICO's over een interne informatiesystemen ('IS ICO') beschikken en dat dit systeem geen algemene en directe toegang geeft aan de Russische autoriteiten tot de data in deze interne informatiesystemen.

Datum
1 april 2026

Ons kenmerk
2025-005323

Volgens Ridetech kunnen de Russische autoriteiten alleen informatie opvragen en kunnen ICO's via de zogenoemde 'HSS ICO' de opgevraagde informatie met de Russische autoriteiten delen. Wat er zij van het niet-onderbouwde en niet te verifiëren standpunt van Ridetech dat Yandex.Taxi LLC en Yandex LLC, als ICO's over een intern informatiesystemen ('IS ICO') beschikken en dat dit systeem geen algemene en directe toegang geeft aan de Russische autoriteiten tot de data in deze interne informatiesystemen, houdt de AP het ervoor dat niet kan worden uitgesloten dat de Russische autoriteiten in de praktijk over bredere toegangsrechten beschikken ten aanzien van de informatiesystemen van Yandex.Taxi LLC en Yandex LLC. Overigens heeft ook Ridetech in haar Transfer Impact Assessment stilgestaan bij de omstandigheid dat de Russische autoriteiten over zeer ruime bevoegdheden van toegang tot persoonsgegevens beschikken en dat in Rusland een reëel risico bestaat op machtsmisbruik en willekeur.⁶⁵ Die door Ridetech zelf opgetekende reflectie, biedt steun voor het oordeel van de AP.

84. Het voorgaande betekent dat Ridetech niet heeft kunnen aantonen dat zij, gelet op de geldende Russische wetgeving, passende waarborgen heeft getroffen om te voorkomen dat Yandex.Taxi LLC en Yandex LLC persoonsgegevens van Finse en Noorse gebruikers van de Yango-app toegankelijk kunnen maken voor de Russische autoriteiten.
85. Gelet op het vorenstaande is de AP van oordeel dat ook na 27 november 2023 Yandex.Taxi LLC en Yandex LLC persoonsgegevens van Finse en Noorse gebruikers van de Yango-app hebben ontvangen zonder dat door Ridetech passende waarborgen in de zin van artikel 46 AVG werden geboden.

5.4.3 Afdwingbare rechten en doeltreffende rechtsmiddelen

86. Een ander vereiste uit artikel 46, eerste lid, AVG waaraan de AP in het kader van passende waarborgen moet toetsen, is of betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken wanneer Ridetech hun persoonsgegevens aan Yandex.Taxi LLC en Yandex LLC in Rusland doorgeeft.
87. Het HvJ EU heeft bepaald dat de doorgifte van persoonsgegevens, door standaardbepalingen, afhankelijk is van de stand van het recht en de praktijk van het betrokken derde land (in dit geval Rusland). Volgens het HvJ EU kunnen zich situaties voordoen waarin de voorschriften van de standaardbepalingen mogelijk onvoldoende zijn om de daadwerkelijke bescherming van de naar het betrokken derde land doorgegeven persoonsgegevens in de praktijk te waarborgen. Dat is met name het geval wanneer het recht van dat derde land de overheidsinstanties van dat land toestaat om in te grijpen in de rechten van de betrokkenen met betrekking tot die gegevens.⁶⁶
88. Standaardbepalingen berusten namelijk op een contract tussen de verwerkingsverantwoordelijke en de ontvanger van persoonsgegevens. Zij zijn dus niet bindend voor de autoriteiten van het derde land waarnaar persoonsgegevens worden doorgegeven. Het is daarom essentieel dat in het land, waar de

⁶⁵ Dossierstuk 86 bij het onderzoeksrapport, p. 46-47.

⁶⁶ HvJ EU 16 juli 2020, [ECLI:EU:C:2020:559](#) (Schrems I), r.o. 126.

Datum
1 april 2026

Ons kenmerk
2025-005323

ontvanger van persoonsgegevens is gevestigd, een onafhankelijke toezichthoudende autoriteit aanwezig is.⁶⁷

89. In paragraaf 2.4 van dit besluit is weergegeven dat de Russische *Roskomnadzor* toezicht houdt op de naleving van privacyregelgeving. *Roskomnadzor* maakt deel uit van het Ministerie van Digitale Ontwikkeling, Communicatie en Massamedia van de Russische Federatie. Bovendien is *Roskomnadzor* belast met het toezicht op de naleving van de Information Act en de zogenoemde ‘*Yarovaya law*’. Op basis van de ‘*Yarovaya law*’ kan *Roskomnadzor* de dienstenverlening van ondernemingen blokkeren die niet voldoen aan genoemde wetgeving. Eén van de verplichtingen die op grond van de ‘*Yarovaya law*’ op de ondertoezichtgestelden rust, is dat zij desgevraagd encryptiesleutels van data aan de Russische autoriteiten moeten overhandigen. De AP stelt vast dat *Roskomnadzor* zowel de toezichthouder is op de bescherming van persoonsgegevens als ook de toezichthouder is op de naleving van de ‘*Yarovaya law*’, dat antiterrorisme wetgeving is en daarmee belangen dient die tegenstrijdig zijn met de belangen die gemeoid zijn met de bescherming van persoonsgegevens.
90. Daar komt bij dat de *European Data Protection Supervisor* een analyse heeft gemaakt naar de toegang tot persoonsgegevens bij doorgifte naar landen buiten de EER.⁶⁸ Daarin is vastgesteld dat de *Roskomnadzor* in de praktijk uitsluitend boetes of waarschuwingen oplegt aan private organisaties en natuurlijke personen⁶⁹, terwijl de bevoegdheden van *Roskomnadzor* tegenover overheidsinstanties niet expliciet benoemd zijn. In dit kader is relevant dat *Roskomnadzor* onder de verantwoordelijkheid valt van het Ministerie van Digitale Ontwikkeling, Communicatie en Massamedia van de Russische Federatie. De AP merkt op dat in het kader van de doorgifte van persoonsgegevens naar Rusland juist de bescherming tegen inmenging door de overheid van wezenlijk belang is. De AP concludeert dat het onafhankelijke toezicht van *Roskomnadzor* op overheidsinstanties niet gewaarborgd is, omdat *Roskomnadzor* ten eerste hiërarchisch ondergeschikt is aan het voornoemde ministerie, ten tweede omdat *Roskomnadzor* uitvoering moet geven aan twee tegenstrijdige belangen (bescherming van persoonsgegevens tegenover antiterrorismewetgeving) en ten derde omdat *Roskomnadzor* haar toezicht kennelijk niet inzet bij de bescherming van persoonsgegevens tegenover overheidsinstellingen. Daarom kan naar het oordeel van de AP niet worden gesteld dat de rechten van betrokkenen voldoende beschermd worden door *Roskomnadzor*.
91. Gelet op het voorgaande is de AP van oordeel dat *Roskomnadzor* niet kan worden aangemerkt als een onafhankelijke toezichthoudende autoriteit in de zin van artikel 45, tweede lid, AVG. Daarmee beschikken betrokkenen dus niet over afdwingbare rechten en doeltreffende rechtsmiddelen, zoals artikel 46, eerste lid, AVG vereist.

⁶⁷ European Commission decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, para. 58.

⁶⁸ EDPS, november 2021, ‘*Government access to data in third countries*’, [EDPS/2019/02-13](#).

⁶⁹ EDPS, november 2021, ‘*Government access to data in third countries*’, [EDPS/2019/02-13](#), p.49.

Datum
1 april 2026

Ons kenmerk
2025-005323

5.5 Eindconclusie

92. De AP heeft vastgesteld dat Ridetech persoonsgegevens van gebruikers van de Yango-app uit de EER verwerkt. Deze persoonsgegevens worden doorgegeven aan Yandex.Taxi LLC, die tezamen met Ridetech geldt als gezamenlijke verwerkingsverantwoordelijke. Die persoonsgegevens worden voorts doorgegeven aan de verwerker, Yandex LLC. Beide ontvangers van de persoonsgegevens zijn gevestigd in Rusland. Daarom mocht de doorgifte van de persoonsgegevens van betrokkenen uit de EER alleen dan plaatsvinden als passende waarborgen geboden werden en als betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikten. Daarvan is naar het oordeel van de AP niet gebleken.
93. Naar oordeel van de AP heeft Ridetech in ieder geval sinds 23 mei 2022 geen passende waarborgen geboden in de zin van artikel 46 AVG. De AP heeft vastgesteld dat in ieder geval tussen 23 mei 2022 en 27 november 2023 persoonsgegevens in versleutelde vorm samen met de bijbehorende encryptiesleutels werden doorgegeven naar Rusland zonder dat passende waarborgen geboden werden. Na 27 november 2023 heeft Ridetech weliswaar maatregelen getroffen, waaronder het opnieuw versleutelen van de persoonsgegevens en het bewaren van de encryptiesleutels binnen de EER, maar zijn deze maatregelen naar oordeel van de AP niet voldoende om een passend beschermingsniveau te bieden aan betrokkenen uit de EER.
94. Daarnaast heeft Ridetech verzuimd aan te tonen dat Russische autoriteiten geen toegang hebben tot persoonsgegevens van betrokkenen die op de servers van Yandex.Taxi LLC en Yandex LLC worden verwerkt. Evenmin beschikken betrokkenen uit de EER over afdwingbare rechten en doeltreffende rechtsmiddelen bij de doorgifte van persoonsgegevens.
95. Dat brengt de AP tot de conclusie dat dat Ridetech persoonsgegevens van betrokkenen uit de EER heeft doorgegeven naar een derde land dat geen passend beschermingsniveau waarborgt. Dit betekent dat betrokkenen uit de EER met deze doorgifte benadeeld worden. Gelet op het voorgaande is de AP van oordeel dat Ridetech in ieder geval vanaf 23 mei 2022 tot op heden in overtreding is van de artikelen 44 en 46 AVG, gelezen in samenhang met artikel 5, eerste lid, onder a, en tweede lid, AVG.
96. Gesteld noch gebleken is dat Ridetech zich kan beroepen op de uitzonderingen van artikel 49 AVG.

6. Bestuurlijke boete

6.1 Boetebevoegdheid

97. De AP is op grond van artikel 58, tweede lid, aanhef en onder i, in verbinding met artikel 83, AVG en gelezen in samenhang met artikel 14, derde lid, UAVG, bevoegd om een bestuurlijke boete op te leggen. Uit de jurisprudentie van het HvJ EU blijkt dat uit de bewoordingen van artikel 83, tweede lid, AVG volgt dat inbreuken op de bepalingen van de AVG die door de verwerkingsverantwoordelijke op verwijtbare wijze

Datum
1 april 2026

Ons kenmerk
2025-005323

zijn begaan – dat wil zeggen opzettelijk of uit nalatigheid begane inbreuken – ertoe kunnen leiden dat aan de verwerkingsverantwoordelijke op grond van dat artikel een administratieve geldboete kan worden opgelegd.⁷⁰

98. De AP heeft vastgesteld dat Ridetech een overtreding heeft begaan van artikelen 44 en 46 AVG in samenhang met artikel 5, eerste lid, onder a en tweede lid, AVG. Ridetech had op grond van de AVG kunnen weten dat zij voor het doorgeven van persoonsgegevens naar ontvangers in Rusland passende waarborgen had moeten treffen. Vanwege deze overtreding en de ernst ervan ziet de AP aanleiding om gebruik te maken van haar bevoegdheid om een bestuurlijke boete op te leggen.

6.2 Systematiek bepalen boetehoogte

99. De EDPB heeft in de plenaire vergadering van 24 mei 2023 ingestemd met de definitieve tekst van de Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG (hierna: de Richtsnoeren).⁷¹ De AP zal deze Richtsnoeren toepassen op deze zaak.⁷²
100. De Richtsnoeren berekening administratieve boetes beschrijven de volgende methode voor het berekenen van administratieve geldboeten voor inbreuken op de AVG:
1. in kaart brengen welke en hoeveel handelingen en inbreuken ter beoordeling voorliggen;
 2. het uitgangsbetrag voor de verdere berekening van de boete bepalen;
 3. nagaan of zich verzachtende of verzwarende omstandigheden zijn die nopen tot verhoging of verlaging van de geldboete;
 4. nagaan welke maximumbedragen gelden voor de overtredingen en of die maximumbedragen niet worden overschreden als gevolg van in voorgaande of volgende stappen toegepaste verhogingen;
 5. nagaan of het berekende eindbedrag van de geldboete voldoet aan de vereisten van effectiviteit, afschrikking en proportionaliteit, en zo nodig de geldboete hieraan aanpassen.

101. Deze stappen worden hierna achtereenvolgens doorlopen.

6.3 Berekening boetebedrag

6.3.1 Stap 1: Vaststellen handelingen en inbreuken

102. Om het startbedrag van de boete te bepalen, moet allereerst worden bezien of sprake is van één of meerdere sanctioneerbare gedragingen.

⁷⁰ HvJ EU 5 december 2023, ECLI:EU:C:2023:949 (*NVSC*) r.o. 73 en 83; HvJ EU 5 december 2023, ECLI:EU:C:2023:950 (*Deutsche Wohnen*) r.o. 68 en 76.

⁷¹ Zie ook Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG.

⁷² Zie ook <https://www.autoriteitpersoonsgegevens.nl/actueel/nieuw-boetebeleid-voor-overtredingen-avg>

Datum
1 april 2026

Ons kenmerk
2025-005323

103. De AP heeft geconstateerd dat er sprake is van één gedraging, namelijk de doorgifte van persoonsgegevens aan ontvangers in Rusland waarvoor een bestuurlijke boete zal worden opgelegd.

6.3.2 Stap 2: Bepalen uitgangsbetrag

104. Vervolgens moet de AP het uitgangsbetrag van de boetehoogte bepalen. Dit bedrag vormt het uitgangspunt voor de verdere berekening in latere stappen, waarbij alle relevante feiten en omstandigheden in aanmerking worden genomen. Het uitgangsbetrag wordt bepaald aan de hand van drie elementen:

- i) de categorisatie van de inbreuken volgens artikel 83, vierde tot en met zesde lid, AVG;
- ii) de zwaarte van de inbreuk; en
- iii) de omzet van de onderneming.

Ad i) Categorisatie van de inbreuken volgens artikel 83, vierde tot en met zesde lid, van de AVG

105. Vrijwel alle verplichtingen van de verwerkingsverantwoordelijke zijn gecategoriseerd in de bepalingen van artikel 83, vierde tot en met zesde lid, AVG. De AVG maakt onderscheid tussen twee soorten inbreuken. Enerzijds de inbreuken die sanctioneerbaar zijn op grond van artikel 83, vierde lid, AVG, en waarvoor een maximumboete geldt van € 10 miljoen (of in geval van een onderneming, 2% van de jaaromzet, indien dat hoger is), anderzijds de inbreuken die sanctioneerbaar zijn op grond van artikel 83, vijfde en zesde lid, AVG, en waarvoor een maximumboete geldt van € 20 miljoen (of in geval van een onderneming, 4% van de jaaromzet, indien dat hoger is). Met dit onderscheid heeft de wetgever voorzien in een eerste indicatie van de zwaarte van de inbreuk: hoe zwaarder de inbreuk, hoe hoger de boete.

106. In dit geval kan de AP een bestuurlijke boete opleggen van maximaal € 20 miljoen (of in geval van een onderneming, 4% van de wereldwijde jaaromzet, indien dat hoger is). Uit deze categorisering volgt dat de inbreuk van deze bepalingen door de wetgever (in abstracto) als ernstig worden gezien.

Ad ii) Zwaarte van de inbreuk

107. Bij het bepalen van de zwaarte van de inbreuk houdt de AP rekening met de aard, ernst en duur van de overtreding, alsmede met de opzettelijke of nalatige aard van de inbreuk en de categorieën betrokken persoonsgegevens.

108. Bij de aard van de inbreuk kijkt de AP naar het belang dat de overtreden bepaling beoogt te beschermen. De AP constateert dat Ridetech de continuïteit van het hoge niveau van de bescherming van de AVG bij doorgifte van persoonsgegevens naar een derde land, niet heeft gewaarborgd. Door het ontbreken van passende waarborgen in de periode van de overtreding, heeft Ridetech persoonsgegevens onbehoorlijk doorgegeven naar ontvangers die Rusland zijn gevestigd. Dit terwijl Rusland een ontoereikend beschermingsniveau heeft, omdat Russische autoriteiten op grond van de lokale wetgeving toegang

Datum
1 april 2026

Ons kenmerk
2025-005323

kunnen krijgen tot persoonsgegevens van betrokkenen uit Noorwegen en Finland. Deze inbreuk vormt een direct gevaar voor het recht op een privéleven en het recht op de bescherming van persoonsgegevens zoals neergelegd in respectievelijk artikel 7 en artikel 8 van het Handvest.

109. Voor wat betreft de ernst van de inbreuk houdt de AP rekening met relevante omstandigheden over de aard, omvang en doel van de verwerking, het aantal betrokkenen en de (eventuele) omvang van de schade.
110. In dit geval kent de AP aan de aard van de verwerking een groot gewicht toe omdat de verwerking Russische autoriteiten in staat stelt om toegang te krijgen in persoonsgegevens van betrokkenen uit Noorwegen en Finland. Ook aan de omvang van de verwerking kent de AP een groot gewicht toe omdat het om grensoverschrijdende verwerking van persoonsgegevens gaat naar een derde land zonder dat daarvoor passende waarborgen zijn getroffen. Verder kent de AP een neutraal gewicht toe aan het doel van de verwerking omdat niet gebleken is op welke wijze de naar Rusland doorgegeven persoonsgegevens ten dienste komen aan de kernactiviteiten van Ridetech in Noorwegen en Finland of de verbetering van de software van de Yango-app.
111. Verder houdt de AP er rekening mee dat van tienduizenden betrokkenen in Noorwegen en Finland de persoonsgegevens aan ontvangers in Rusland zijn doorgegeven.
112. Ook weegt de AP mee dat de inbreuk in ieder geval vanaf 23 mei 2022 heeft plaatsgevonden en dat de inbreuk nog steeds voortduurt. De overtreding heeft dan ook een lange duur.
113. Tot slot weegt de AP mee dat met de onderhavige verwerking veel categorieën van persoonsgegevens zijn gemoeid (zie randnummers 20 en 20). Bij de verwerking van persoonsgegevens van chauffeurs zijn ook sociale zekerheidsnummers en foto's onderdeel van de verwerking geweest. Dit zijn gevoelige persoonsgegevens die extra bescherming behoeven..

Ad iii) Omzet van de onderneming

114. De AP relateert een billijk uitgangsbetrag van de boete aan de grootte van de onderneming. De grootte van de onderneming wordt bepaald aan de hand van de omzet. Het uitgangsbetrag voor een kleine onderneming is lager en het uitgangsbetrag neemt toe naar mate de omzet van de onderneming hoger is. Indien een onderneming een omzet heeft van meer dan € 500 miljoen, geldt dat de boetehoogte wordt bepaald op een percentage van de jaaromzet van de onderneming.⁷³ Hierdoor is de grootte en omzet van de onderneming reeds verdisconteerd in de hoogte van de boete, zodat het uitgangsbetrag geen aanpassing op die grond behoeft.
115. Zoals vermeld in overweging 150 van de AVG, moet bij het opleggen van een boete aan een onderneming de “onderneming” worden gezien als een onderneming overeenkomstig de artikelen 101 en 102 van het Verdrag betreffende de werking van de Europese Unie. Uit vaste jurisprudentie van het HvJ EU volgt dat

⁷³ Vanaf een jaaromzet van € 500 miljoen geldt dat 4% van de jaaromzet hoger is dan € 20 miljoen, zodat dit percentage als boetemaximum in aanmerking moet worden genomen (artikel 83, vijfde lid, aanhef, van de AVG).

Datum
1 april 2026

Ons kenmerk
2025-005323

een onderneming elke eenheid is die een economische activiteit uitoefent, ongeacht haar rechtsvorm en de wijze waarop zij wordt gefinancierd. Het gaat dus om de economische eenheid van de onderneming en niet om de juridische entiteiten daarbinnen. Verschillende vennootschappen of entiteiten binnen dezelfde economische eenheid kunnen dus samen een onderneming zijn in de zin van voormelde bepalingen.

116. Ridetech was, totdat zij op 24 oktober 2025 werd ontbonden, een volledige dochteronderneming van MLU B.V. die op haar beurt (via Y.E. Holding Limited uit de Verenigde Arabische Emiraten en Y.E. Holding d.o.o. Beograd uit Servië) een dochteronderneming is van de Russische Consortium.First die via IPJSC YANDEX beursgenoteerd is aan de aandelenbeurs van Moskou. De AP rekent deze ondernemingen voor de toepassing van artikel 83 van de AVG tot dezelfde economische eenheid.
117. IPJSC YANDEX heeft de jaarstukken over 2024 op haar website gepubliceerd.⁷⁴ De wereldwijde omzet van de onderneming over 2024 bedraagt volgens die publicatie 1.094,6 miljard Russische Roebels. Dat komt overeen met € 12,08 miljard.⁷⁵
118. Op grond van artikel 83, vijfde lid, van de AVG bedraagt het boetemaximum 4% van de jaaromzet. Uitgaande van de jaaromzet van € 12,08 miljard, bedraagt het boetemaximum voor de overtreding € 483,2 miljoen.
119. De waardering van de hiervoor aangehaalde omstandigheden en factoren bepaalt de algehele ernst van de inbreuk begaan door Ridetech. Het gaat daarbij om een grondige beoordeling van de concrete omstandigheden van het geval waarin alle omstandigheden in samenhang moeten worden gezien.
120. Gelet op hetgeen onder i) en ii) is overwogen, is de AP van oordeel dat het niveau van zwaarte van de inbreuk moet worden gekwalificeerd als "hoog". Volgens de Richtsnoeren geldt voor inbreuken met een hoog niveau van ernst, dat het uitgangsbetrag dient te worden bepaald op een punt tussen 20% en 100% van het boetemaximum van in dit geval € 483,2 miljoen. Dit komt overeen met een bedrag tussen de € 96,6 miljoen en € 483,2 miljoen. Daarbij geldt als algemene regel dat hoe ernstiger de inbreuk binnen zijn eigen categorie is, hoe hoger het uitgangsbetrag zal zijn.
121. De AP is van oordeel dat, gelet op de omschreven omstandigheden, de inbreuk ernstig is.
122. Op basis van de categorisatie van de inbreuk, de zwaarte van de inbreuk en de omzet van de onderneming stelt de AP het uitgangsbetrag voor de onderhavige overtreding vast op € 100 miljoen.

6.3.3 Stap 3: Beoordelen overige relevante omstandigheden

Vervolgens moet de AP vaststellen of in de omstandigheden van het geval er aanleiding is om de boete hoger of lager vast te stellen dan het hiervoor bepaalde startbedrag. De in aanmerking te nemen omstandigheden zijn vermeld in artikel 83, tweede lid, aanhef en onder a tot en met k, AVG. De in die

⁷⁴ Te raadplegen via [Financials 2024](#) | [Investor Relations](#) | [Yandex](#)

⁷⁵ Wisselkoers van 31 maart 2026: 100 Russische Roebels = € 1,07.

Datum
1 april 2026

Ons kenmerk
2025-005323

bepaling vermelde omstandigheden moeten elk slechts eenmaal worden gezien. In de vorige stap heeft de AP reeds rekening gehouden met de zwaarte van de overtreding (onderdeel a), de opzettelijke of nalatige aard van de inbreuk (onderdeel b) en de categorieën van persoonsgegevens (onderdeel g). Daardoor resteren nog de onderdelen c tot en met f en h tot en met k.

123. De enige van toepassing zijnde omstandigheid is de wijze waarop de AP kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke de inbreuk heeft gemeld (onderdeel h). In dit geval heeft Ridetech de inbreuken niet zelf gemeld, maar is de AP via de Noorse en Finse privacytoezichthouders op de hoogte geraakt van de onderhavige inbreuk. Dit wordt volgens de Richtsnoeren echter als “neutraal” beoordeeld en heeft daarom geen gevolgen voor de hoogte van de op te leggen boete.

6.3.4 Stap 4: relevante maximumbedragen

124. Gelet op de omzet van moederonderneming van Ridetech zal voor de geconstateerde overtreding een maximum boetehoogte van 4% van de wereldwijde jaaromzet van de onderneming gelden. De jaaromzet bedraagt € 12,08 miljard, zodat het boetemaximum voor de overtreding € 483,2 miljoen bedraagt.
125. Op grond van de bovenstaande overwegingen stelt de AP het boetebedrag voor de geconstateerde overtreding vast op € 100 miljoen. Dit ligt onder het wettelijk maximum zodat zich geen overschrijding daarvan voordoet.

6.3.5 Stap 5: Beoordeling vereisten van doeltreffendheid, evenredigheid en afschrikking

126. Tot slot beoordeelt de AP of de boete doeltreffend, evenredig en afschrikkend zijn. Ook op grond van de artikelen 3:4 en 5:46, tweede lid, Algemene wet bestuursrecht mag de bestuurlijke boete, gezien de omstandigheden van het concrete geval, niet tot een onevenredige uitkomst leiden. Dit is ook neergelegd in artikel 49 van het Handvest.
127. Zoals in de Richtsnoeren omschreven, kan het opleggen van een boete als effectief worden beschouwd als deze het doel bereikt waarvoor deze is opgelegd. Dat doel kan zijn gelegen in enerzijds het bestraffen van onrechtmatige gedragingen en anderzijds het bevorderen van naleving van de geldende voorschriften.
128. Gelet op alle in artikel 83, tweede lid, AVG genoemde factoren, zoals hiervoor beoordeeld, is de AP van oordeel dat het opleggen van een bestuurlijke boete van € 100 miljoen onder deze omstandigheden evenredig, doeltreffend en afschrikkend is. De overtreding kan Ridetech worden verweten.

Datum
1 april 2026

Ons kenmerk
2025-005323

7. Verwerkingsverbod

129. De AP besluit om op grond van artikel 58, tweede lid, aanhef en onder f, AVG met ingang van de datum van dit besluit een verbod op te leggen aan MLU B.V. Dat verbod houdt in dat het MLU B.V. niet is toegestaan doorgifte te laten plaatsvinden van persoonsgegevens van Noorse en Finse gebruikers van de Yango-app aan de ontvangers in Rusland.
130. Het doel van het verwerkingsverbod is om de nog voortdurende overtreding te beëindigen. De AP wijst er volledigheidshalve op dat het niet naleven van het verwerkingsverbod zelfstandig kan worden beboet. Daartoe is de AP op grond van artikel 83, vijfde lid, aanhef en onder e, AVG bevoegd.

8. Besluit

- De AP legt aan MLU B.V., die na ontbinding van Ridetech alle rechten en plichten van Ridetech heeft overgenomen, wegens overtreding van artikelen 44 en 46 AVG in samenhang met artikel 5, eerste lid, onder a en tweede lid, AVG, in de periode vanaf 23 mei 2022 tot en met heden, een bestuurlijke boete op van € 100.000.000.⁷⁶

- De AP legt aan MLU B.V., die na ontbinding van Ridetech alle rechten en plichten van Ridetech heeft overgenomen, met onmiddellijke ingang een verwerkingsverbod op voor doorgifte van persoonsgegevens van Noorse en Finse gebruikers van de Yango-app naar ontvangers in Rusland.

Hoogachtend,
Autoriteit Persoonsgegevens,

W.G.

mr. A. Wolfsen
voorzitter

⁷⁶ De AP zal voornoemde vordering uit handen geven aan het Centraal Justitieel Incassobureau (CJIB).



Datum
1 april 2026

Ons kenmerk
2025-005323

Rechtsmiddelenclausule

Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens. Ingevolge artikel 38 van de UAVG schort het indienen van een bezwaarschrift de werking van de beschikking tot oplegging van de bestuurlijke boete op. Voor het indienen van digitaal bezwaar, zie www.autoriteitpersoonsgegevens.nl, onder het kopje Contact, item “Bezwaar of klacht over de AP”.⁷⁷

Het adres voor het indienen op papier is:

Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ Den Haag.

Vermeld op de envelop ‘Awb-bezwaar’ en zet in de titel van uw brief ‘bezwaarschrift’.

Schrijf in uw bezwaarschrift ten minste:

- uw naam en adres;
- de datum van uw bezwaarschrift;
- het in deze brief genoemde kenmerk (zaaknummer), of voeg een kopie van dit besluit bij;
- de reden(en) waarom u het niet eens bent met dit besluit;
- uw handtekening.

⁷⁷ De directe URL is <<https://www.autoriteitpersoonsgegevens.nl/over-de-autoriteit-persoonsgegevens/bezwaar-maken>>.

Datum
1 april 2026

Ons kenmerk
2025-005323

Bijlage 1

Algemene verordening gegevensbescherming

Artikel 4

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

- 1) „persoonsgegevens”: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
- 2) „verwerking”: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
- 3) „beperken van de verwerking”: het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken
- 4) „profilering”: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;
- 5) „pseudonimisering”: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;
- 6) „bestand”: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;
- 7) „verwerkingsverantwoordelijke”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en

Datum
1 april 2026

Ons kenmerk
2025-005323

de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

- 8) „verwerker”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
- 9) „ontvanger”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;
- 10) „derde”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;
- 11) „toestemming” van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;
- 12) „inbreuk in verband met persoonsgegevens”: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
- 13) „genetische gegevens”: persoonsgegevens die verband houden met de overgeërfdde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon;
- 14) „biometrische gegevens”: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;
- 15) „gegevens over gezondheid”: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;
- 16) „hoofdvestiging”:
 - a) met betrekking tot een verwerkingsverantwoordelijke die vestigingen heeft in meer dan één lidstaat, de plaats waar zijn centrale administratie in de Unie is gelegen, tenzij de beslissingen over de doelstellingen van en de middelen voor de verwerking van persoonsgegevens worden genomen in een andere vestiging van de verwerkingsverantwoordelijke die zich eveneens in de Unie

Datum
1 april 2026

Ons kenmerk
2025-005323

bevindt, en die tevens gemachtigd is die beslissingen uit te voeren, in welk geval de vestiging waar die beslissingen worden genomen als de hoofdvestiging wordt beschouwd;

b) met betrekking tot een verwerker die vestigingen in meer dan één lidstaat heeft, de plaats waar zijn centrale administratie in de Unie is gelegen of, wanneer de verwerker geen centrale administratie in de Unie heeft, de vestiging van de verwerker in de Unie waar de voornaamste verwerkingsactiviteiten in het kader van de activiteiten van een vestiging van de verwerker plaatsvinden, voor zover op de verwerker krachtens deze verordening specifieke verplichtingen rusten;

17) „vertegenwoordiger”: een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening;

18) „onderneming”: een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen;

19) „concern”: een onderneming die zeggenschap uitoefent en de ondernemingen waarover die zeggenschap wordt uitgeoefend;

20) „bindende bedrijfsvoorschriften”: beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meer derde landen binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen;

21) „toezichthoudende autoriteit”: een door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie;

22) „betrokken toezichthoudende autoriteit”: een toezichthoudende autoriteit die betrokken is bij de verwerking van persoonsgegevens omdat:

a) de verwerkingsverantwoordelijke of de verwerker op het grondgebied van de lidstaat van die toezichthoudende autoriteit is gevestigd;

b) de betrokkenen die in de lidstaat van die toezichthoudende autoriteit verblijven, door de verwerking wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; of

c) bij die toezichthoudende autoriteit een klacht is ingediend;

23) „grensoverschrijdende verwerking”:

a) verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd; of

Datum
1 april 2026

Ons kenmerk
2025-005323

b) verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden;

24) „relevant en gemotiveerd bezwaar”: een bezwaar tegen een ontwerpbesluit over het bestaan van een inbreuk op deze verordening of over de vraag of de voorgenoemde maatregel met betrekking tot de verwerkingsverantwoordelijke of de verwerker strookt met deze verordening, waarin duidelijk de omvang wordt aangetoond van de risico's die het ontwerpbesluit inhoudt voor de grondrechten en de fundamentele vrijheden van betrokkenen en, indien van toepassing, voor het vrije verkeer van persoonsgegevens binnen de Unie;

25) „dienst van de informatiemaatschappij”: een dienst als gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad;

26) „internationale organisatie”: een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.

Artikel 5

1. Persoonsgegevens moeten:

- a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie”);
- b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding”);
- c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking”);
- d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren („juistheid”);
- e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen („opslagbeperking”);

Datum
1 april 2026

Ons kenmerk
2025-005323

f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid”).

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen („verantwoordingsplicht”).

Artikel 44

Persoonsgegevens die worden verwerkt of die zijn bestemd om na doorgifte aan een derde land of een internationale organisatie te worden verwerkt, mogen slechts worden doorgegeven indien, onverminderd de overige bepalingen van deze verordening, de verwerkingsverantwoordelijke en de verwerker aan de in dit hoofdstuk neergelegde voorwaarden hebben voldaan; dit geldt ook voor verdere doorgiften van persoonsgegevens vanuit het derde land of een internationale organisatie aan een ander derde land of een andere internationale organisatie. Alle bepalingen van dit hoofdstuk worden toegepast opdat het door deze verordening voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd.

Artikel 46

1. Bij ontstentenis van een besluit uit hoofde van artikel 45, lid 3, mag een doorgifte van persoonsgegevens aan een derde land of een internationale organisatie door een verwerkingsverantwoordelijke of een verwerker alleen plaatsvinden mits zij passende waarborgen bieden en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken.

2. De in lid 1 bedoelde passende waarborgen kunnen worden geboden door de volgende instrumenten, zonder dat daarvoor specifieke toestemming van een toezichthoudende autoriteit is vereist:

- a) een juridisch bindend en afdwingbaar instrument tussen overheidsinstanties of -organen;
- b) bindende bedrijfsvoorschriften overeenkomstig artikel 47;
- c) standaardbepalingen inzake gegevensbescherming die door de Commissie volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure zijn vastgesteld;
- d) standaardbepalingen inzake gegevensbescherming die door een toezichthoudende autoriteit zijn vastgesteld en die door de Commissie volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure zijn goedgekeurd;
- e) een overeenkomstig artikel 40 goedgekeurde gedragscode, samen met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of de verwerker in het derde land om de passende waarborgen, onder meer voor de rechten van de betrokkenen, toe te passen; of
- f) een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme, samen met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of de verwerker in het derde land om de passende waarborgen, onder meer voor de rechten van de betrokkenen, toe te passen.

3. Onder voorbehoud van de toestemming van de bevoegde toezichthoudende autoriteit kunnen de in lid 1 bedoelde passende waarborgen ook worden geboden door, met name: a) contractbepalingen tussen de

Datum
1 april 2026

Ons kenmerk
2025-005323

verwerkingsverantwoordelijke of de verwerker en de verwerkingsverantwoordelijke, de verwerker of de ontvanger van de persoonsgegevens in het derde land of de internationale organisatie; of b) bepalingen die moeten worden opgenomen in administratieve regelingen tussen overheidsinstanties of -organen, waaronder afdwingbare en effectieve rechten van betrokkenen.

4. De toezichthoudende autoriteit past het in artikel 63 bedoelde coherentiemechanisme toe in de in lid 3 van dit artikel vermelde gevallen.

5. Toestemmingen die een lidstaat of een toezichthoudende autoriteit op grond van artikel 26, lid 2, van Richtlijn 95/46/EG heeft verleend, blijven geldig totdat zij door die toezichthoudende autoriteit, indien nodig, worden gewijzigd, vervangen of ingetrokken. De besluiten die de Commissie op grond van artikel 26, lid 4, van Richtlijn 95/46/EG heeft vastgesteld, blijven van kracht totdat zij bij een overeenkomstig lid 2 van dit artikel vastgesteld besluit van de Commissie, indien nodig, worden gewijzigd, vervangen of ingetrokken.

Artikel 58

1. Elk toezichthoudende autoriteit heeft alle volgende onderzoeksbevoegdheden om:

- a) de verwerkingsverantwoordelijke, de verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke of van verwerker te gelasten alle voor de uitvoering van haar taken vereiste informatie te verstrekken;
- b) onderzoeken te verrichten in de vorm van gegevensbeschermingscontroles;
- c) een toetsing te verrichten van de overeenkomstig artikel 42, lid 7, afgegeven certificeringen;
- d) de verwerkingsverantwoordelijke of de verwerker in kennis te stellen van een beweerde inbreuk op deze verordening; e) van de verwerkingsverantwoordelijke en de verwerker toegang te verkrijgen tot alle persoonsgegevens en alle informatie die noodzakelijk is voor de uitvoering van haar taken; en
- f) toegang te verkrijgen tot alle bedrijfsruimten van de verwerkingsverantwoordelijke en de verwerker, daaronder begrepen tot alle uitrustingen en middelen voor gegevensverwerking, in overeenstemming met het uniale of lidstatelijke procesrecht.

2. Elk toezichthoudende autoriteit heeft alle volgende bevoegdheden tot het nemen van corrigerende maatregelen:

- a) de verwerkingsverantwoordelijke of de verwerker waarschuwen dat met de voorgenomen verwerkingen waarschijnlijk inbreuk op bepalingen van deze verordening wordt gemaakt;
- b) de verwerkingsverantwoordelijke of de verwerker berispen wanneer met verwerkingen inbreuk op bepalingen van deze verordening is gemaakt;
- c) de verwerkingsverantwoordelijke of de verwerker gelasten de verzoeken van de betrokkene tot uitoefening van zijn rechten uit hoofde van deze verordening in te willigen;
- d) de verwerkingsverantwoordelijke of de verwerker gelasten, waar passend, op een nader bepaalde manier en binnen een nader bepaalde termijn, verwerkingen in overeenstemming te brengen met de bepalingen van deze verordening;

Datum
1 april 2026

Ons kenmerk
2025-005323

- e) de verwerkingsverantwoordelijke gelasten een inbreuk in verband met persoonsgegevens aan de betrokkene mee te delen;
- f) een tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod, opleggen;
- g) het rectificeren of wissen van persoonsgegevens of het beperken van verwerking uit hoofde van de artikelen 16, 17 en 18 gelasten, alsmede de kennisgeving van dergelijke handelingen aan ontvangers aan wie de persoonsgegevens zijn verstrekt, overeenkomstig artikel 17, lid 2, en artikel 19;
- h) een certificering intrekken of het certificeringsorgaan gelasten een uit hoofde van de artikelen 42 en 43 afgegeven certificering in te trekken, of het certificeringsorgaan te gelasten geen certificering af te geven indien niet langer aan de certificeringsvereisten wordt voldaan;
- i) naargelang de omstandigheden van elke zaak, naast of in plaats van de in dit lid bedoelde maatregelen, een administratieve geldboete opleggen op grond van artikel 83; en
- j) de opschorting van gegevensstromen naar een ontvanger in een derde land of naar een internationale organisatie gelasten.

3. Elke toezichthoudende autoriteit heeft alle autorisatie- en adviesbevoegdheden om:

- a) de verwerkingsverantwoordelijke advies te verstrekken in overeenstemming met de procedure van voorafgaande raadpleging van artikel 36;
- b) op eigen initiatief dan wel op verzoek, aan het nationaal parlement, aan de regering van de lidstaat, of overeenkomstig het lidstatelijke recht aan andere instellingen en organen alsmede aan het publiek advies te verstrekken over aangelegenheden die verband houden met de bescherming van persoonsgegevens;
- c) toestemming te geven voor verwerking als bedoeld in artikel 36, lid 5, indien die voorafgaande toestemming door het lidstatelijke recht wordt voorgeschreven;
- d) overeenkomstig artikel 40, lid 5, advies uit te brengen over en goedkeuring te hechten aan de ontwerpgedragscodes;
- e) certificeringsorganen te accrediteren overeenkomstig artikel 43;
- f) certificeringen af te geven en certificeringscriteria goed te keuren overeenkomstig artikel 42, lid 5;
- g) de in artikel 28, lid 8, en artikel 46, lid 2, punt d), bedoelde standaardbepalingen inzake gegevensbescherming aan te nemen;
- h) toestemming te verlenen voor de in artikel 46, lid 3, punt a), bedoelde contractbepalingen;
- i) toestemming te verlenen voor de in artikel 46, lid 3, punt b), bedoelde administratieve regelingen;
- j) goedkeuring te hechten aan bindende bedrijfsvoorschriften overeenkomstig artikel 47.

4. Op de uitoefening van de bevoegdheden die uit hoofde van dit artikel aan de toezichthoudende autoriteit worden verleend, zijn passende waarborgen van toepassing, daaronder begrepen doeltreffende voorziening in rechte en eerlijke rechtsbedeling, zoals overeenkomstig het Handvest vastgelegd in het Unierecht en het lidstatelijke recht.

Datum
1 april 2026

Ons kenmerk
2025-005323

5. Elke lidstaat bepaalt bij wet dat zijn toezichthoudende autoriteit bevoegd is inbreuken op deze verordening ter kennis te brengen van de gerechtelijke autoriteiten en, waar passend, daartegen een rechtsvordering in te stellen of anderszins in rechte op te treden, teneinde de bepalingen van deze verordening te doen naleven.

6. Elke lidstaat kan bij wet bepalen dat zijn toezichthoudende autoriteit, naast de in lid 1, 2 en 3 bedoelde bevoegdheden bijkomende bevoegdheden heeft. De uitoefening van die bevoegdheden doet geen afbreuk aan de doeltreffende werking van hoofdstuk VII.

Artikel 83

1. Elke toezichthoudende autoriteit zorgt ervoor dat de administratieve geldboeten die uit hoofde van dit artikel worden opgelegd voor de in de leden 4, 5 en 6 vermelde inbreuken op deze verordening in elke zaak doeltreffend, evenredig en afschrikkend zijn.

2. Administratieve geldboeten worden, naargelang de omstandigheden van het concrete geval, opgelegd naast of in plaats van de in artikel 58, lid 2, onder a) tot en met h) en onder j), bedoelde maatregelen. Bij het besluit over de vraag of een administratieve geldboete wordt opgelegd en over de hoogte daarvan wordt voor elk concreet geval naar behoren rekening gehouden met het volgende:

a) de aard, de ernst en de duur van de inbreuk, rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade;

b) de opzettelijke of nalatige aard van de inbreuk;

c) de door de verwerkingsverantwoordelijke of de verwerker genomen maatregelen om de door betrokkenen geleden schade te beperken;

d) de mate waarin de verwerkingsverantwoordelijke of de verwerker verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd overeenkomstig de artikelen 25 en 32;

e) eerdere relevante inbreuken door de verwerkingsverantwoordelijke of de verwerker;

f) de mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;

g) de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft;

h) de wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke of de verwerker de inbreuk heeft gemeld;

i) de naleving van de in artikel 58, lid 2, genoemde maatregelen, voor zover die eerder ten aanzien van de verwerkingsverantwoordelijke of de verwerker in kwestie met betrekking tot dezelfde aangelegenheid zijn genomen;

Datum
1 april 2026

Ons kenmerk
2025-005323

j) het aansluiten bij goedgekeurde gedragscodes overeenkomstig artikel 40 of van goedgekeurde certificeringsmechanismen overeenkomstig artikel 42; en

k) elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende factor, zoals gemaakte financiële winsten, of vermeden verliezen, die al dan niet rechtstreeks uit de inbreuk voortvloeien.

3. Indien een verwerkingsverantwoordelijke of een verwerker opzettelijk of uit nalatigheid met betrekking tot dezelfde of daarmee verband houdende verwerkingsactiviteiten een inbreuk pleegt op meerdere bepalingen van deze verordening, is de totale geldboete niet hoger dan die voor de zwaarste inbreuk.

4. Inbreuken op onderstaande bepalingen zijn overeenkomstig lid 2 onderworpen aan administratieve geldboeten tot 10 000 000 EUR of, voor een onderneming, tot 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is: a) de verplichtingen van de verwerkingsverantwoordelijke en de verwerker overeenkomstig de artikelen 8, 11, 25 tot en met 39, en 42 en 43; b) de verplichtingen van het certificeringsorgaan overeenkomstig de artikelen 42 en 43; c) de verplichtingen van het toezichthoudend orgaan overeenkomstig artikel 41, lid 4.

5. Inbreuken op onderstaande bepalingen zijn overeenkomstig lid 2 onderworpen aan administratieve geldboeten tot 20 000 000 EUR of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is:

- a) de basisbeginselen inzake verwerking, met inbegrip van de voorwaarden voor toestemming, overeenkomstig de artikelen 5, 6, 7 en 9;
- b) de rechten van de betrokkenen overeenkomstig de artikelen 12 tot en met 22;
- c) de doorgiften van persoonsgegevens aan een ontvanger in een derde land of een internationale organisatie overeenkomstig de artikelen 44 tot en met 49;
- d) alle verplichtingen uit hoofde van krachtens hoofdstuk IX door de lidstaten vastgesteld recht;
- e) niet-naleving van een bevel of een tijdelijke of definitieve verwerkingsbeperking of een opschorting van gegevensstromen door de toezichthoudende autoriteit overeenkomstig artikel 58, lid 2, of niet-verlening van toegang in strijd met artikel 58, lid 1.

6. Niet-naleving van een bevel van de toezichthoudende autoriteit als bedoeld in artikel 58, lid 2, is overeenkomstig lid 2 van dit artikel onderworpen aan administratieve geldboeten tot 20 000 000 EUR of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

7. Onverminderd de bevoegdheden tot het nemen van corrigerende maatregelen van de toezichthoudende autoriteiten overeenkomstig artikel 58, lid 2, kan elke lidstaat regels vaststellen betreffende de vraag of en in hoeverre administratieve geldboeten kunnen worden opgelegd aan in die lidstaat gevestigde overheidsinstanties en overheidsorganen.

8. De uitoefening door de toezichthoudende autoriteit van haar bevoegdheden uit hoofde van dit artikel is onderworpen aan passende procedurele waarborgen overeenkomstig het Unierecht en het lidstatelijke recht, waaronder een doeltreffende voorziening in rechte en eerlijke rechtsbedeling.

Datum
1 april 2026

Ons kenmerk
2025-005323

9. Wanneer het rechtsstelsel van de lidstaat niet voorziet in administratieve geldboeten, kan dit artikel aldus worden toegepast dat geldboeten worden geïnitieerd door de bevoegde toezichhoudende autoriteit en opgelegd door bevoegde nationale gerechten, waarbij wordt gewaarborgd dat deze rechtsmiddelen doeltreffend zijn en eenzelfde effect hebben als de door toezichhoudende autoriteiten opgelegde administratieve geldboeten. De boeten zijn in elk geval doeltreffend, evenredig en afschrikkend. Die lidstaten delen de Commissie uiterlijk op 25 mei 2018 de wetgevingsbepalingen mee die zij op grond van dit lid vaststellen, alsmede onverwijld alle latere wijzigingen daarvan en alle daarop van invloed zijnde wijzigingswetgeving.

Uitvoeringswet Algemene verordening gegevensbescherming

Artikel 14

Taken en bevoegdheden AP

[...]

3. De Autoriteit persoonsgegevens kan in geval van overtreding van het bepaalde in artikel 83, vierde, vijfde of zesde lid, van de verordening een bestuurlijke boete opleggen van ten hoogste de in deze leden genoemde bedragen.