Aker Solutions Privacy Statement for Aker Security Services

This Privacy Statement represents the privacy policy applicable to Aker Solutions ASA ("Aker Solutions") when acting as sole or joint controller as defined by Article 4(7) of Regulation (EU) 2016/679 (GDPR) when collecting, using and disclosing personal data about customers´ employees and other personnel, visitors of the customer, offenders, suspected offenders and members of the public entering the immediate vicinity of an area that is subject to the security services provided by Aker Solutions.

Aker Solutions has established a security service offering covering their facilities and operations in the majority of the countries they operate in ("Aker Security Services"). The services are offered to customers out across the Aker Group to assist and enable a unified security approach for efficiency and professional development across the entities. The same services are offered to customers which are not members of the Aker Group to meet service requests from such customers. Aker Solutions will partly deliver the services with in-house personnel and partly with third party service providers.

Members of the Aker Group are defined as companies in which Aker ASA or The Resource Group TRG AS, directly or indirectly, through ownership of shares or other financial instruments holds in excess of 30% of the share capital or votes of the company, whilst also being the largest shareholder of the company based on share capital or votes.

If you have any questions relating to this Privacy Statement please contact Aker Solutions' Global Security Operations Center ("GSOC") at gsoc@akersolutions.com or Aker Solutions ASA, Oksenøyveien 8, NO-1366 Lysaker, Norway.

1 HOW AND WHY WE USE PERSONAL DATA

Personal data is processed as part of delivering the Aker Security Services to customers of Aker Solutions for the purposes set out in this Privacy Statement. The Aker Security Services are either part of a bundle package or delivered as a single service depending on customers' needs. The Aker Security Services may e.g. consist of the following activities:

- **Monitoring** (general surveillance through the security systems used):
    - **remote alarm monitoring** such as monitoring of doors both inside and outside of facilities and of alarms that go off in a building/site. In this context, information about the cause of the alarm is processed from video surveillance, access control and intruder alarm logs, hereunder personal data of the person(s) involved in the incident and in events that occur before or after the event;
    - **internal event monitoring** such as monitoring of social events with internal and/or external participants. In this context, information about the participants (their name,

contact information, role and employer) collected from the participant's employer or the participant itself is processed, together with information from video surveillance and access control logs related to the security of the event and other information related to the security threat posed to the specific event;

- **remote video monitoring of premises and activity logs from access control systems, etc.** In this context, information from CCTV placed on the premises in question is processed. This includes surveillance cameras with analytics. Such surveillance cameras are uniquely designed and configured to support the environment where they are placed and linked to risk assessments that define the operational requirements for each such camera. They work both reactively and proactively and have capabilities like self-learning video analytics, license plate recognition, appearance search and focus of attention. Such cameras may for example be used to detect cars with a license plate that are registered to an individual that on the basis of a risk assessment constitutes risk to Aker Solutions or its customers, or in order to detect in a short time persons invading a building being secured by Aker Solutions, by searching through the system or surveillance cameras with analytics. From the access control system, the same information as listed below regarding cardholder administration (collected through the Service Portal or through an HR integration with the customer's HR systems) may be processed in relation to remote video monitoring.

- **Critical event management** such as monitoring of global incidents that could pose a threat to the security and safety of customers and their employees, information, infrastructure and assets. In this context, information from various public sources like news channels, media, public social media platforms, and other sources such as security intelligence databases and similar platforms is processed, some of which may contain personal data relating to the name of the person that may pose a threat to the relevant Customers and other personal information made publicly available related to the threat. This also includes identifying which people or assets might be at risk and if they are safe, in light of the information detected by the critical event management platform, the PNR Feeds from Aker Solutions' and the customers' travel management provider which are part of the service Track and Communicate and our security systems such as for access control.

    - **risk center** where data from over 20,000 open sources worldwide is collected and used to alert GSOC when something happens near one of the customers' assets, so that GSOC can access, locate and take action. With more complete intelligence, customers will be able to increase their response time an decisiveness in order to assess risks safeguard their employees from harm from such risks or disrupting their operations. Risk center is contextual data from open source systems and an enabler for GSOC to respond and provide targeted real-time alerting to customers'

employees of domestic and worldwide incidents and events, dramatically increasing the ability to respond to risks that threaten people and organizations both globally and locally. Information from risk center is used for form a basis for the events that employees of customers are informed of through Safety Connection, Mass notification and Track and Communicate.

- **Safety Connection** where any time employees of customers log onto the customers' network, swipe an access badge or voluntarily download the Safety Connection mobile app (which processes exact location if this functionality is turned on), it is captured by Safety Connection, which provides a dynamic location to make sure that the concerned employees are provided with as accurate and relevant information as possible with regards to threats to their safety in light of their real time location. In addition, static location information from Aker Solutions' HR systems, PNR feeds from the customers' and Aker Solutions' travel management provider, check-ins from the employee through the Safety Connection mobile app, access badge information based on use of access bade to a facility or based on IT network location login information is processed and when combined with direct access to the leading intelligence feeds, this allows GSOC to monitor active threats in relation to their people's safety and automatically alert them when they are close to or approaching danger. Two-way communication capabilities further allow recipients to acknowledge receipt of alerts, confirm their safety or request additional assistance. The mobile SOS button and Safe Corridor feature allows customers' employees to notify when they need help, or voluntarily check-in, when they feel they are in a potentially dangerous situation. In this regard first name, last name, work email, employee ID, company, work country code, segment/business area/business unit, work phone, private phone, private e-mail and PNR feed may be processed.

- **Mass notification** with incident communications where customers can send emergency communications through an emergency management application to their employees through their work phone or work phone SMS, private phone or private phone SMS, company email, private email, satellite phone if available, IT system with desk top alerts or through the Safety Connection mobile app, keeping them informed before, during and after critical events.

- **Travel safety and security**

  - **Track and Communicate** when employees are travelling for work globally.
    In this context, information about hotels, rental cars and flights and the mobile geolocation of the employee is processed if the employee decides to share such

information with Aker Solutions by enabling such function through the relevant application. Communication with the employee relating to travel safety and security can be through e-mail, SMS, satellite phone, mobile phone, land line and Aker Solutions' notification systems over internet.

- This information is collected from a customer representative through the Service Portal, through Aker Solutions' and the customers' travel management provider or through an HR integration with the customer's HR and travel systems and the employee's mobile phone (if geolocation is enabled) and is combined with information from critical event management in order to monitor and safeguard the safety of the employees when travelling as described above.

- As a part of Track and Communicate, so-called PNR feeds from Aker Solutions travel management provider are processed relating to the individual employees. PNR feeds contain information such as employee ID, employment status, first name, last name, corporate email address, work country, code, business unit ID, company ID, travel payment options (mandatory), and may in addition include information such as travel policy options, middle name, name prefix, date of birth, gender, mobile number country code, work address, cost center ID, department name, employment start and end date and position (voluntary).

- **Active monitoring of people and assets in high/extreme risk countries** through GPS tracking of location, such as through satellite phones, apps and GPS tracking devices, etc., as further explained before such tracking is initiated for the specific employee.

  Executive protection such as remote video monitoring and remote alarm monitoring of private households where the same data is processed as for remote video monitoring of premises and activity logs from access control systems, etc. and for remote alarm monitoring as further described in Aker ASA Executive Protection Protocol.

- **Emergency response** (emergency phone & dispatch, etc.)

  - **Receipt, handling and dispatch of emergency calls** to relevant lines.
    In this context, information about the name of the caller, name of people involved in the incident and other personal information related to the emergency in question is processed to the extent necessary for the emergency response. The emergency calls may be recorded for safety and training purposes.

- **Cardholder administration**

    - **access cards, activity logs from access control systems, credential, access management, etc**. In this context, the information listed below is collected through the relevant access control system, from a customer representative through the Service Portal and/or an HR integration with the customer's HR systems, or directly from the individual in question (sometimes when applying for a new access card).

    - When applying for a new access card, the following information is processed:
        - First name, middle name, last name
        - Company
        - Employee ID
        - Card type
        - Location, building, zone
        - End date
        - Send access card to
        - Email, alternative email
        - Telephone number
        - Date of birth
        - Photo

    - When the registration process is completed the following attributes are created and linked to your personal profile:
        - Badge ID and UID number
        - Employee ID and/or tenant employee ID
        - Company (legal entity)

    - As a part of using the access card, information about when and where the card is used will be processed (information from activity logs from access control system, log from canteen payment system etc.). This includes information from systems that are integrated with the access control system, such as printers, canteen, event registration, evacuation, vending machines, etc., depending on the customer's choices and where the employee uses his/her access card.

- **Digital ID**

    - **Mobile access card** where the employee's mobile device is used as an access card. In this context, picture of the employee is processed (collected through HR integrations, receptions, photo booths or from the employee's device), ID-numbers

for the digital-ID, together with the information referred to above relating to cardholder administration.

- Pictures for digital ID are either collected through HR integrations or taken in a photo booth or by the reception in question, and uploaded to the Service Portal and then linked to the employee's profile when ordering a new access card or taking a new picture.

- When pictures are taken in such photo booth, consent is obtained from the employee to Aker Solutions' use of the picture. Such consent can be withdrawn at any time by following the contact information provided in the consent form.

- **Technical security systems/security technology, etc**.

  - **The underlying systems that support the services described above** process various categories of personal data, such as access logs, pictures from CCTV, activity logs in information systems, manual logs, GPS-location data, name, contact information, employee number, name of employer, manager and a picture of the employee, etc.

  - **Integrations** where certain personal data is disclosed from the customer containing a selected set of data depending on the integration in question. Many of the integrations are so-called HR integrations, but the main integrations is the HR feed where data categories such as first name, last name, phone number (work and private), email (work and private), employee ID, company, work country code, travel payment option ID, travel policy group ID and segment/business area/business unit are mandatory data categories. In addition, certain other data categories such as travel policy options, middle name, name prefix, date of birth, gender, country code, work address, cost center ID, department name, employment start and end date and position (voluntary) may be processed as additional elements decided upon jointly between the customer and Aker Solutions.

    Depending on the customers' preferences, the HR feed may either consist merely of the mandatory elements, or any additional elements chosen by the customer. If and to the extent Aker Solutions and the customers jointly decide on parts of the integrations, the parties act as joint controllers for such processing. For more information on such processing, see point 1.1 below or contact your Aker Group company.

  - **Data insight** where interactive dashboards are created to gain deeper insights into the data processed for the customer when delivering the Aker Security Services, such as for infection control purposes, calculating investment cost and other legitimate

and necessary purposes. In this context, relevant data collected as part of the Aker Security Services is used in order to create aggregated data dashboard with numbers and trends for the customer. For example, data from the cardholder administration may be used in order to create a dashboard for the customer with an aggregated overview over how many employees went in and out of a building, to ensure compliance with applicable infection control regulations, and similar purposes. The customer can create and arrange multiple charts and text elements on the dashboard, create filters for viewing specific data, and create drilldowns to let the customer change the detail level of data displayed, always at an aggregated level.

- **Training** where various categories of personal data may be processed as a part of providing relevant staff with training in the software applications used to provide the different services described. Personal data will only be processed to the extent necessary as a part of such training, for example when providing staff with training in how to use video surveillance systems or relevant access control systems.

- **Reception and related tasks, etc.**

  - **Reception personnel** processes personal data to the extent necessary to conduct the tasks required by the reception, such as to provide access to employees, conduct limited monitoring of the premises through CCTV, assist visitors and conduct other administrative tasks.

  - In order to fulfil these tasks, reception personnel has access to cardholders' profile on the Service Portal and the information referred to above relating to cardholder administration.

- **Guarding and guest management systems, etc.**

  - When visitors register in the guarding and guest management systems, information about the visitor's name, telephone, company, e-mail and who they are visiting is collected directly from the visitor upon registration. Information about the person being visited is collected from Aker Solutions HR-system.

  - Such personal data is collected with the consent of the visitor, that may be withdrawn at any time by following the information provided in the consent form.

- **Related services and consulting services** (building projects, new site establishment, analysis & assessments, governance, training, investigations and design specifications).

- With regard to building projects, new site establishment and training, information about the full name, telephone number, employee number is processed. This information is collected either through the Service Portal or through HR integrations.

- With regard to analysis & assessments, name and contact information is collected through the Service Portal.

Personal data will also be processed as part of the administration of the services mentioned above, e.g. as part of administering and using the Service Portal.

Personal data processed will typically relate to customer's employees and other personnel (including when travelling), visitors of the customer, offenders, suspected offenders and members of the public e.g. those entering or in the immediate vicinity of the area under video surveillance.

As a main rule, the processing of personal data described above will be based on the legitimate interests pursued by the controller which are not overridden by the interests or the fundamental rights and freedoms of the data subject, cf. GDPR Article 6 (1) letter f. For more information about the legitimate interests being pursued by the controller, please see sections 1.1 and 1.2 below.

Aker Solutions will also process personal data to the extent necessary to comply with legal obligations.

- Such obligations may for example involve processing of personal data necessary to comply with tax and accounting obligations, obligations relating to work environment and health, social security and processing of other information relating to legal proceedings and insurance incidents.
- The purpose and legal basis for such processing is to comply with legal obligations to which Aker Solutions is subject and Aker Solutions' legitimate interests in the establishment, exercise or defence of legal claims and/or to protect a legal position of Aker Solutions.

In some cases, Aker Solutions processes personal data with the data subject's consent which may be withdrawn at any time by following the instructions in the applicable consent form, as described above.

1.1 Where Aker Security Services are delivered to an Aker Group company

Where Aker Security Services are delivered to a customer in the Aker Group, Aker Solutions acts as an independent controller for the processing of personal data that takes place as part of the services for the following purposes and for the following legitimate interests:

- providing an appropriate level of security and support and the best possible services
- ensuring that people, information, infrastructure and assets are protected through an holistic approach throughout the Aker Group
- resource management and internal control

- improving and developing Aker Solutions' services
- analytics.

Aker Solutions and the Aker Group company acting as customer, are joint controllers for processing that takes place for integrations and data flows that the parties have agreed upon jointly in the event and to the extent such processing takes place as part of the services. For further information regarding such processing, you should contact the Aker Group company acting as data controller jointly with us.

1.2 Where Aker Security Services are delivered to a non-Aker Group company

Where Aker Security Services are delivered to a customer which is not a member of the Aker Group, Aker Solutions acts as an independent controller or the processing of personal data that takes place as part of the services for the purposes of and for the following legitimate interests:

- improving and developing the services
- analytics
- providing the best possible services to customer.

Aker Solutions and the customer act as joint controllers for processing that takes place as part of the services for the purposes of providing an appropriate level of security and support and for ensuring that people, information, infrastructure and assets are protected and for integrations and data flows that the parties have agreed upon jointly, in the event and to the extent such processing takes place. For further information regarding such processing, you should contact the relevant non-Aker Group company acting as data controller jointly with us.

2 SHARING OF PERSONAL DATA

We will not share your personal data with third parties except for in circumstances where such sharing is necessary to provide our services, to achieve our business objectives or as further described in this section.

Personal data processed for purposes for which Aker Solutions and the customer act as joint controllers, cf. section 1.1 and 1.2 above, will be shared between the parties, to the extent necessary for the purposes.

Where necessary or required by legal obligations to which we are subject, personal data is shared with employees and agents, services providers, data subjects, police forces, security organisations and persons making an inquiry, provided that such inquiry complies with applicable law.

We use third-party service providers to deliver the services on our behalf and on our instructions as set out in a data processing agreement with the relevant service provider. We use such service providers for example for our Service Portal, customer satisfaction surveys, for delivering systems and related support, IT security services and monitoring, hosting websites and performing statistical analysis of our services, for HR and financial administration and for communication. In such instances, we may share your personal data with such parties to the extent necessary for the service provider to perform the agreed services.

When necessary for delivering the Aker Security Services, we may share your personal data with other Aker Group companies and/or business units, for example where the customer is a member of the Aker Group or if we use other Aker Group companies to provide the services on our behalf. We also share your personal data with other Aker Group companies for example in instances where the Aker Group company in question is the customer of the Aker Security Services, in order to fulfill the agreement with the customer.

When required by law, regulation, legal process or an enforceable governmental request, we may share your personal data for legal reasons to public authorities or governments but only to the extent we are required to do so.

As part of carrying out specific projects in collaboration with our business partners we may share personal data with such parties to the extent necessary to carry out such projects.

We will not disclose your personal data to third parties for the purposes of allowing them to market their products or services to you, nor will we disclose personal data to our carefully selected business partners, unless there is legal basis for such disclosure and other requirements in applicable law are complied with.

3 TRANSFER OF PERSONAL DATA

When sharing personal data to other parties as described above, we sometimes need to transfer personal data to a country outside the EEA in order to be able to fulfil one of the purposes set out in this Privacy Statement. As an example, transfer of personal data may take place when we are using service providers outside the EEA in order to be able to perform the services mentioned in section 2 paragraph 4 and when we provide our services to customers outside the EEA or to global customers.

We will not transfer personal data to a third country outside of the EEA that does not provide adequate protection of personal data unless appropriate safeguards are adduced or the transfer otherwise takes place in accordance with applicable data protection legislation. Examples of such appropriate safeguards are Binding Corporate Rules and EU Standard Contractual Clauses.

Aker Solutions will sometimes, as a part of providing the services, transfer personal data from Aker Solutions to other Aker Group companies outside the EU/EEA to the extent necessary to provide the services (for example when the customer is a member of the Aker Group). Aker Solutions has adopted binding corporate rules for processing and transfer of personal data ("Aker Solutions Data Protection Procedure", "BCR") which provide a legal basis for transferring personal data from Aker Group companies established within the EU/EEA to Aker Group companies established outside the EU/EEA. The BCR have been approved by the Norwegian and other relevant data protection authorities and are an important measure to ensure and demonstrate compliance with GDPR. For more information about the BCR and group companies bound by the BCR, please see http://www.akersolutions.com.

4 SECURITY OF PROCESSING

We will process your personal data securely and will apply and maintain appropriate technical and organizational measures to protect your personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Access to personal data is strictly limited to personnel of Aker Solutions and its controlled business units and affiliates who have appropriate authorization and a clear business need for that data.

5 RETENTION AND DELETION OF DATA

Your personal data will be retained as long as necessary to fulfil the legitimate purpose(s) for the processing and as long as required by law. We determine retention periods based on the legitimate needs of the business to deliver its services.

If you request us to perform services on your behalf, we will retain your personal data for as long as necessary to perform those services as further described in our internal procedure on retention periods.

6 YOUR RIGHTS AS A DATA SUBJECT

You have the right to request access to and rectification of any information we have collected about you. To help us keep your personal data updated, we advise you to inform us of any changes or discrepancies you believe are relevant.

You also have the right to erasure and restriction of processing in some instances. You may have a right to receive personal data concerning you in a machine-readable format and to forward the data to another party (data portability), provided that certain conditions are met.

You also have the right to object to processing that relies on legitimate interests as a legal basis. In order to object to processing, please contact the Global Security Operations Center at gsoc@akersolutions.com.

If and to the extent we process personal data with your consent, you have the right to withdraw such consent at any time. Note that withdrawal of consent does not affect the lawfulness of a processing that takes place prior to the withdrawal of consent.

To exercise your rights as a data subject, or if you wish to make a complaint regarding our compliance with this Privacy Statement or our BCR, please contact the Global Security Operations Center at gsoc@akersolutions.com. We prefer requests to be filed in writing. Prior to fulfilling your request, we may ask you to:

a) Specify the IT system in which the personal data are likely to be stored;
b) Specify the circumstances in which we obtained the personal data; and
c) Show proof of your identity.

Further, in cases of access requests, we may ask you to specify the categories of personal data that you request access to.

You have a right to complain to the Norwegian Data Protection Authority, but we encourage you to first contact the Group Privacy Officer, before filing such complaint.

7 PRIVACY STATEMENTS OF THIRD PARTIES

This Privacy Statement addresses the collection, use and disclosure of personal data by Aker Solutions as described above. This Privacy Statement does not address or govern the privacy practices adopted by third parties on third party websites or in relation to third party services.

Although we try only to link to websites that share our high standards for privacy, we are not in any way responsible for the content or the privacy practices employed by third party websites or third party services. We encourage you to familiarize yourself with the privacy policies applicable to such websites or services prior to providing them with your personal data.

8 GOVERNING LAW AND JURISDICTION

This Privacy Statement applies to all customers of the Aker Security Services. The rights and obligations of Aker Solutions and its customers are entirely governed by Norwegian law.

This shall however not in any way limit the data subjects' right to lodge a complaint with a supervisory authority in the member state of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data under this Privacy Statement infringes applicable data protection law.

9 CHANGES TO THIS PRIVACY STATEMENT

We may update this Privacy Statement from time to time. If such updates are minor and do not have a material meaning for your rights or the way we use personal data, we may make such changes

without posting a specific notice on our website. We encourage you to review this Private Statement on a regular basis to familiarize yourself with the latest updates.

If we make material changes to this Privacy Statement that may affect your rights or the way we use personal data, we will provide a specific notice on our website and/or other relevant channels.

10 HOW TO CONTACT US

If you have any questions or comments relating to this Privacy Statement or want to exercise your rights, please contact the Group Privacy Officer.

Effective date: [1/9-2021] / **Last updated:** [1/9-2021]