# AKJ General Data Privacy and Protection Policy

- AK JENSEN GROUP -



June 2022

## 1. Definitions

The following definitions are to be used when reading this policy.

***"AKJ"*** refers to all entities within AKJ Group.

***"GDPR"*** is defined as The European Union General Data Protection Regulation No. 2016/679.

***"Personal data"*** is defined as any information relating to an identified or identifiable natural person – including name, address, ID number, location data, but also online identifiers such as cookies and IP addresses. It can also relate to one or more factors specific to the physical, physiological, genetic, mental, economic cultural or society identity of that natural person

***"Data Subject"/ "data subject" / "data subject"***: means an individual who is the subject of personal data.

***"Processing"*** is defined in Article 4(2) of the GDPR and includes almost any operation or set of operations which is performed on Personal Data including collection, recording, organization, structuring, storage, adaptation, disclosure by transmission use and deletion. A ***Processor*** covers any natural or legal person who processes Personal Data on behalf of a controller.

A ***"Controller"*** is defined under Article 4(7) of the GDPR and covers any natural or legal person which determines the purpose and means of the processing of particular personal data, and usually collects the data.

***"We", "us", "AKJ", "our"*** refers to AK Jensen Investment Management Limited

***"Sensitive Personal Data"*** is classed as a special category data under Article 9 GDPR and relates to information concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.

Please note that AKJ does not process any ***sensitive personal data*** on a large scale as defined by GDPR.

"***Lawful basis"*** relates to the particular lawful basis that has been selected for the processing of data as is required by GDPR (there are six - consent; contract; legal obligation; vital interests; public task; legitimate interests)

***"Data Protection Officer (DPO)"***- The GDPR introduces a duty to appoint a DPO if you are a public authority, or if you carry out certain types of processing activities.

Please note that AKJ does not technically need to appoint a DPO and will not formally appoint one - the Compliance function will be responsible in the first instance for all DP matters.

***"The Principles"*** are the six data protection principles that govern the processing of all data.

**"Data subject Rights"** are the rights that data subjects have under GDPR for example to erasure, correction, accuracy.

## 2. Introduction

GDPR applies across the EEA and UK with effect from 25 May 2018 and outlines the requirements behind the processing of Personal Data and the free movement of such data. Personal Data will be subject to processing and controlling in accordance with Article 6 of GDPR by AKJ and our third-party

service providers and their delegates, authorized agents and associated or affiliated companies within the European Union.

On the 14th April 2016, the EU approved a new legal framework called GDPR which aims to allow individuals to take back control of their Personal Data. GDPR has principally come about as a result of social and economic integration across the world, rapid technology developments and globalisation all of which has meant that our Personal Data is shared much more widely than even before. In addition, although there already existed data protection law which came from a European Directive, it was left to each member state to interpret and implement which resulted in disparate local data protection laws across the continent. As a result there was a need to create a strong, more coherent data protection framework backed by robust enforcement.

In the UK, The Data Protection Act 1998 put a lot of onus on Data Controllers to take responsibility for the Personal Data they hold. The GDPR tightens these regulations but also puts much greater onus on Data Processors to maintain records of Personal Data and processing activities too. Brexit will not affect implementation in the UK as the UK government has stated the legislation will be adopted regardless of the UK status within the EEA.

There are new and extended provisions in GDPR that either did not existing under previous DP law in the EEA and UK, or were not sufficiently robust, which include:

- The right to be forgotten – if people no longer want their data stored they can ask for it to be deleted in certain circumstances.
- The right to data portability – people can ask for their data in certain formats so they can take it with them if they change service provider for example.
- The requirement to gain explicit consent if one processes any sensitive personal data such as medical or health information, religious or sexual orientation.
- Tighter requirements around the reporting of breaches of data protection requirements, and the reporting of these.

AKJ is committed to complying fully with GDPR, and that all its employees are aware of the requirements and obligations to ensure that data subjects privacy is not invaded going forward.

GDPR places a great emphasis on firms documenting and recording their approach to protecting data and AKJ will in all cases comply with this need to maintain robust documentation and records.

One of the main aims of GDPR is to encourage firms to make their employees aware of their obligations under the new Regulation, and AKJ will carry out appropriate awareness and other training for its employees.

## 3. Personal Data and the legal basis for processing such data

AKJ may collect from data subjects and process Personal Data of the kind that can be found on the below unexhaustive list:

- name
- email
- utility bill and address
- passport
- CVs
- AKJ FIT questionnaire (requesting for certain confirmations such as criminal offences and bankruptcies)

- FCA Form A (for applications to FCA for SM functions)
- personal numbers (or equivalent local ID)
- personal trading statements (from external brokers when specifically requested for investigative purposes or when trading outside of AKJ)
- bank details
- Lexus Nexus searches.
- Phone recordings
- IP address
- Investor Categorisation
- cookies

AKJ has undertaken a data inventory/mapping exercise to ascertain for example what categories of data it holds; where it is held; security arrangements in place; where the data is sent to; relevant retention periods; and the lawful basis for holding each data category. This exercise is to be undertaken at least every three years.

Data can only be processed by AKJ if there is a lawful basis for this processing, and there are six such bases that can be used under Article 6 of GDPR for such processing – see below.

**N.B.** Processing of Personal data by AKJ will take place on the basis of being in compliance with a legal obligation and/or on the basis of a contractual necessity and/or consent, and/or legitimate interests.

1) **Consent -** is one lawful basis AKJ can use for processing data, and explicit consent can also legitimise the use of special category data/sensitive personal data. However, It is preferable to use a lawful basis other than consent to process data as the implications of having to use consent are more onerous on data controllers and processors, and the regulatory body in the UK, the Information Commissioner's Office ("ICO") has encouraged firms to try and use one of the other five lawful bases available.

   ICO states "*Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."*

   Please note, AKJ will only use this basis if for example contract, lawful obligation or legitimate interests are not appropriate for the particular circumstances.

2) **Contract** – AKJ have this lawful basis for processing data if the processing is necessary (i.e. there is no other way of achieving what the individual wants without our processing their data), and:

   - AKJ have a contract with the individual and need to process their personal data to comply with our obligations under the contract.
   - AKJ have not yet got a contract with the individual, but they have asked us to do something as a first step (e.g. provide a quote for a brokerage service) and we need to process their personal data to do what they ask.

It does not apply if AKJ need to process one person's details but the contract is with someone else. It also does not apply if AKJ take pre-contractual steps on our own initiative or at the request of a third party.

If AKJ process on the basis of contract, the individual's right to object and right not to be subject to a decision based solely on automated processing will not apply. AKJ will rely on this legal basis when for example entering into discussions and conversations with potential clients, and where Personal Data is collected as part of this.

3) **Legal Obligation** – AKJ can rely on this lawful basis if we need to process the Personal Data to comply with a common law or statutory obligation, i.e. comply with the law. This does not apply to contractual obligations. The processing must be necessary, and if AKJ can reasonably comply without processing the personal data, this basis does not apply.

Regulatory requirements qualify as a legal obligation for these purposes where there is a statutory basis underpinning the regulatory regime and which requires regulated organisations to comply. So AKJ will rely on this lawful basis where we are required to obtain and hold data to comply with regulators requirements (e.g. the FCA in the UK, Finanstilsynet in Norway), and if we need to undertake due diligence when taking on new customers to demonstrate compliance with anti-money laundering regulations.

If AKJ process data on the basis of legal obligation, the data subject has no right to erasure, right to data portability, or right to object.

4) **Vital Interests** – AKJ could rely on vital interests as a lawful basis if we were to need to process the Personal Data to protect someone's life. The processing must be necessary, and if one can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply. One cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

**It is highly unlikely that AKJ will ever rely on this lawful basis,** and vital interests are intended to cover only interests that are essential for someone's life. So this lawful basis is very limited in its scope, and generally only applies to matters of life and death, e.g. hospitals admissions.

5) **Public Task** – AKJ can rely on this lawful basis if we were to need to process Personal Data:

    a. 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or b. to perform a specific task in the public interest that is set out in law.

It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.

**It is highly unlikely that AKJ will ever rely on this lawful basis.**

6) **Legitimate Interests** – is the most flexible lawful basis for processing, but AKJ cannot assume it will always be the most appropriate. It is likely to be most appropriate where AKJ use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. Where AKJ choose to rely on legitimate interests, we are taking on extra responsibility for considering and protecting people's rights and interests.

There are three elements to the legitimate interests basis, and it helps to think of this as a three-part test. AKJ will perform and document this test whenever this legal basis is to be used so as to assess its applicability in the particular circumstances. AKJ need to:

    a. identify a legitimate interest;

b. show that the processing is necessary to achieve it; and

c. balance it against the individual's interests, rights and freedoms.

The legitimate interests can be AKJ's own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits. The processing must be necessary. If AKJ can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

AKJ must balance our interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override AKJ's legitimate interests.

AKJ will rely on this exemption when for example contacting potential business partners who have provided their contact details, perhaps by exchange of business cards – these parties have provided their details with a view to possible future contact on relevant opportunities that may be of interest, and so contact may be expected. Any such contact (e.g. by email or post) using this lawful basis will still provide the data subject with the opportunity to advise AKJ that they do not wish to be contacted again.

## 4. Personal Data through AKJ's website and other electronic means

When visiting AKJ's website https://www.akj.com/ AKJ may collect personal information on you that you voluntarily provide to us as a result of either:

### a. sending a query via the website contact form or via email

When sending a query via the website contact form or via email, visitors are voluntarily providing personal information of the following kind:

- Name Company Name
- Email
- Telephone number
- Country where resident
- Background and track record

The AKJ website features a contact form for request of information. Upon submission, the above data is transmitted

- via email to AKJ
- Via Zapier (integration service) to AKJs Asana

The Contact Form also contains a check button ("*I agree to receive relevant newsletters from AKJ*"), which has as a purpose of explicitly asking for your consent in the event that you wish for further information about AKJ. The check button is off by default.

Any other information the visitor may choose to share with AKJ via the contact form is up to the website visitor.

Unless the visitor has checked the "*I agree to receive relevant newsletters from AKJ"* button and/ or provided such explicit requests to AKJ, AKJ may not and will not use the personal data the visitor provided other than to answer his/her query.

## b. filling out the investor categorization link

When filling out the investor categorization link, the visitor is voluntarily providing personal information of the following kind:

- Name
- Company Name
- Email
- Telephone number
- Country resident
- IP Address (to ensure that multiple requests are not performed by the same one person)
- Investor Categorisation

Such information will be processed by AKJ to ensure that you meet the necessary regulatory MiFID II categorization of a professional investor or equivalent, as well as get confirmation from the visitor (as the case may require) that his/her request comes at his/her own initiative, in order for AKJ to be able to process the visitor's request and send the requested fund information to him/her.

## c. visiting our website https://www.akj.com/

We gather on an **automated basis** technical data when visitors visit AKJ's website such as cookies and IP addresses.

**Cookies**
Website visitors may choose to accept or not the cookie use policy as stated on https://www.akj.com/ by clicking on the cookie notification bar that is displayed upon entering the website.

AKJ's website uses both permanent and temporary session cookies. Temporary session cookies are only stored during your session on the website and deleted when you close down your web browser. A permanent cookie is a text file stored on your computer. Please find below a description of the types of cookies that are in existence:

Process – Process cookies help make a website function and deliver the services that the website visitor expects to receive, such as navigation, access to secure areas etc. These cookies are necessary and without them the website will not function properly.

Preference – Preference cookies allow a website to remember a user's preferences in relation to the website such as language, font size, currency, region etc. These cookies are not vital but enhance a user's experience.

Security – Security cookies are used to authenticate users, prevent fraudulent use of login credentials, protect user data from unauthorised parties etc. These cookies are vital to the security of AKJ's website.

Analytics – Analytics cookies collect information in an anonymous form about how a user interacts with a website. This information may include: the number of users visiting the website, the pages a user visits the activity of the user on the website and how often the user returns.

**How to change a cookie setting**

In order to control cookie settings and delete as applicable, website visitors would have to access the settings section in his/her web browser. Within the settings section, there will be a sub-section called "privacy and security" or similar depending on the browser that they use. From there one can control and delete as applicable saved cookies.

More information about cookies, please go to: allaboutcookies.org

**IP addresses**
Upon visiting AKJ's website, our servers will record visitors' IP address together with the date and time of their visit. An IP address is an assigned number, similar to a telephone number, which allows a computer to communicate over the internet. We will use the visitors' information for demographic and statistical purposes, including to determine the number of visitors to our websites in any given period, and to analyze patterns of use of our websites.

### d. clicking on one of AKJ's advertisements (such as text ads, web banners) used in online advertising.

The personal data we collect from visitors clicking on online advertisements, as defined under the GDPR, are cookie files and IP addresses.

AKJ online ads are displayed on Google browsers and on other publishers' websites according to Google's algorithms that take into account Campaign and Budget settings. Except Campaign default settings as defined by Google and selected by AKJ, AKJ has no influence on how and where the online ads will be displayed.

In its capacity of online advertiser by means of Google's AdWords Platform and Account, AKJ is subject to Google's Privacy Policy and Terms of Use on all associated Google Platforms. https://policies.google.com/privacy?hl=en.

## 5. Personal data from telephone recordings

All telephone conversations and electronic communications between you and us may be recorded and retained by us, and will be recorded where those conversations or communications, result or may result in the conclusion of a transaction in accordance with all relevant statutory or other regulatory requirements for such period specified from time to time in the applicable Regulations. Such records shall constitute conclusive evidence of the conversations, instructions or orders recorded.

## 6. The Data Protection Principles

AKJ is classed as a Data Controller and also a Processor under GDPR. This statement confirms our commitment to protect data subjects privacy and to process data subjects Personal Data in accordance with the regulations. Such data will be processed and protected in accordance with GDPR's 7 principles in Article 5 of the regulation as detailed below:

**I. Lawfulness, fairness, and transparency**

Personal Data will be processed lawfully, fairly and in a transparent manner.

**II. Purpose limitations**

Personal Data is to collected for a specified, explicit and legitimate purpose and will not be processed for any other purpose that is incompatible with that specified purpose, except where any specific exception applies (e.g. required disclosure to a regulatory authority).

### III. Data minimization

Personal Data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. AKJ will ensure that data held is not excessive.

### IV. Accuracy

Personal Data needs to be accurate and where necessary kept up to date. AKJ will take every reasonable step to ensure that Personal Data is not inaccurate, having regard to the purposes for which it is processed, and thereafter erased or rectified without delay if applicable.

### V. Storage limitations

Personal Data is kept in a form that permits identification of data subjects for no longer than is necessary for the processing purpose(s).

### VI. Integrity and confidentiality

Personal Data is processed in a manner that ensures appropriate security of the data using appropriate technical or organization measures, including against unauthorized or unlawful processing, accidental loss, destruction or damage.

### VII. Accountability

AKJ as controller is responsible for compliance with the Principles and has to be able to demonstrate that processing activities are compliant with these.

## 7. Transfer of Personal data

Transfer of Personal Data provided to any country including countries outside the European Economic Area ("EEA") which may not have equivalent data protection laws to those in the data subject's jurisdiction, may take place for any of the purposes described in this policy. Where this is the case, we will put appropriate safeguards in place to protect the transferred Personal Data in accordance with the General Data Protection Regulation 2016/679, including the use of standard contractual clauses or such other methods as we consider appropriate for such transfers.

Due diligence will be undertaken by AKJ on the security arrangements of any party to whom we transfer Personal Data whether they be within the EEA or outside. Those within the EEA should be fully compliant with all provisions of the GDPR, and also countries outside the area who control or process Personal Data relating to data subjects within the EEA should be similarly compliant. However, it is accepted that the latter may not always be the case, and indeed even the former will be potentially dependant on the veracity with which particular state regulators seek to enforce the regulation.

Inquiries made by AKJ of countries outside the EEA will necessarily need to be more robust – for example any transfers to the US will mean inquiries made as to whether they belong to the Privacy Shield scheme in the US, and if not more detailed diligence as to how they protect personal data.

**Contracts**

All contractual agreements that relate to contracts where Personal Data can be transferred will be checked by AKJ to ensure they contain all GDPR required clauses relating to Personal Data:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject;
- the obligations and rights of the controller;
- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract;
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state;
- state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and
- reflect any indemnity that has been agreed.

## 8. Confidentiality & security

AKJ will take customary and reasonable precautions to maintain the confidentiality of all Personal Data by ensuring that its personnel engaged with processing of Personal Data is provided with the requisite training in relation to GDPR and the importance of confidentiality.

Robust cyber security arrangements will be maintained at all times by AKJ to prevent the risk of data being lost or intercepted. Please see our separate cyber-security policy for details.

Levels of access within AKJ to Personal Data will be continually reviewed to ensure that only those individuals who require access to such data to perform their roles within AKJ, have such access. Where levels of access can be reasonably restricted and do not unduly interfere with the lawful processing of any Personal Data, then such restriction will occur.

The data subjects are advised and need to acknowledge and agree that we may disclose from time to time Personal Data to our other offices, branches, subsidiaries, affiliates, units and Associated Companies, where this is required for purposes relevant to their providing us with this data.

## 9. Retention, Subject Access Requests, return and deletion of data

**Retention Periods**

AKJ and its third-party providers shall ensure that Personal Data is retained in accordance with the applicable regulations and/or in accordance with GDPR as applicable. No Personal Data will be retained indefinitely, but there may be regulatory and legislative requirements that mean AKJ will need to keep such data so as to be able to demonstrate compliance with applicable rules, e.g. those of the Financial Conduct Authority ("FCA") in the UK and also for tax reporting related purposes.

AKJ will ensure that only data strictly relevant to any regulatory and legislative requirement is kept and that any data which can be viewed as peripheral will be destroyed where this is appropriate.

**Subject Access Requests ("SARS")**

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why AKJ are using their data, and check we are doing it lawfully.

Individuals have the right to obtain the following from AKJ:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information – this largely corresponds to the information that AKJ should provide in our privacy notice(see below)

An individual is only entitled to their own Personal Data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, AKJ will establish whether the information requested falls within the definition of Personal Data.

In addition to a copy of their Personal Data, ALKJ will provide individuals with the following information:

- the purposes of the processing;
- the categories of Personal Data concerned;
- the recipients or categories of recipient AKJ disclose the Personal Data to;
- AKJ's retention period for storing the Personal Data or, where this is not possible, our criteria for determining how long we will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing, as is appropriate according to the legal basis used to process the data;
- the right to lodge a complaint with the ICO or another national supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling) if relevant; and
- the safeguards AKJ provide if we transfer personal data to a third country or international organisation.

AKJ provide much of this information already in our privacy notice, which is available on our website and is also provided when Personal Data is collected.

The GDPR does not specify how to make a valid request for a SAR, and therefore, an individual can make a subject access request to AKJ verbally or in writing. It can also be made to any part of our organisation (including by social media) and does not have to be to a specific person or contact point.

A request to AKJ does not have to include the phrase 'subject access request', as long as it is clear that the individual is asking for their own personal data. This means any AKJ employee could receive a valid request. However, AKJ have a legal responsibility to identify that an individual has made a request to AKJ and handle it accordingly, and therefore all such requests should be transferred to the Compliance Department.

A log of all such SARs is maintained in Compliance Department. AKJ will act on the SAR without delay and at the latest within one month of receipt, and this period will be calculated from the day after AKJ receive the request (working day or not) until the corresponding calendar date in the next month.

In most cases AKJ will not charge a fee to comply with a SAR, unless the request is manifestly unfounded or excessive when AKJ may charge a “reasonable fee” for the administrative costs of complying with the request. AKJ can also charge a reasonable fee if an individual requests further copies of their data following a request, and this fee will be based on the administrative costs of providing such further copy.

AKJ will promptly respond to a request by a Data Subject to view and/or return and/or delete its data.

## 10. Data subject rights

AKJ will take all appropriate measures and make available to data subjects information retained on them as required in the applicable legislation.

Data subjects shall have a right to rectify inaccurate Personal Data concerning them and have the right to request for the erasure of Personal Data concerning them.

Data subjects further have the right to object to any Data Processing in accordance with article 18 of the GDPR (this will be dependent on which legal basis you are basing the processing on).

Data subjects have the right to lodge a complaint with AKJ in relation to AKJ’s use of Personal Data by sending an email to compliance@akj.com or with the relevant supervisory authority under the General Data Protection Regulation 2016/679 which shall be the Information Commissioner’s Office (https://ico.org.uk/) in the UK or the equivalent national regulator in any EU country.

## 11. Data Subject Consent

As detailed previously, it is not necessary for AKJ to receive consent from all data subjects, and AKJ will rely on the lawful bases of Contract, Legitimate Interests and Legal Obligation in most cases. AKJ will however, particularly when marketing and relying on Legitimate Interests as the lawful basis for communicating with industry contacts, provide such individuals with the opportunity to elect not to receive any further marketing, information, etc going forward.

AKJ will need express consent when processing special category/sensitive personal data and this includes:

- race
- ethnic origin
- politics
- religion
- trade union membership

- genetics
- biometrics (for ID purposes)
- health
- sex life
- sexual orientation

AKJ will allocate a lawful basis for processing such data, and also need a condition from Article 9 of the GDPR to apply, which for AKJ is obtaining the data subjects' consent.

AKJ will wherever practicable ask data subjects to specifically authorise that we may use, store or otherwise process any Personal Data in according with GDPR (whether provided electronically or otherwise) and may disclose any such Data (including, without limitation, information relating to data subject transactions and accounts) either as we or any of our relevant Associated Companies shall be obliged or requested to under or pursuant to any Applicable Rules or by any regulatory authority (including any tax authority) or as may be required to administer GDPR, in order to provide services to the data subject.

**Children**

Children need particular protection when AKJ collect and process their personal data because they may be less aware of the risks involved. AKJ need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option.

AKJ will try and rely on consent as the lawful basis for processing personal data, and only children aged 16 or over are able provide their own consent.

## 12. Breaches of data protection rules

The GDPR introduces a more onerous and far-reaching regime with respect to breach notification than has previously been the position. AKJ must notify the relevant supervisory authority without undue delay (and certainly within 72 hours of becoming aware of a breach), unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

AKJ's notification will include at least:

- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of the AKJ contact point;
- the likely consequences of the data breach; and measures taken or proposed by the AKJ to address the breach and/or mitigate its effects.

**Communication of a Personal Data breach to the data subject (Article 34)**

Where a Personal Data breach is likely to result in a high risk to the rights and freedoms of a data subject, AKJ as the controller will communicate the breach to the data subject without undue delay. The communication will describe in clear and plain language, the nature of the breach and at least: the name and contact details of the relevant AKJ contact point; the likely consequences of the data breach; and measures taken or proposed by AKJ to address the breach and/or mitigate its effects.

AKJ do not have to make a notification to the data subject where any of the following conditions have been met:

Technical and organisational measures have been applied to the Personal Data which will render it unintelligible to unauthorised persons (such as encryption); AKJ has taken steps to ensure the originally high risk is no longer likely to materialise; or to notify each data subject would involve disproportionate effort, in which case a public communication or other method of information is used which would inform the affected data subjects in similarly effective manner.

Where AKJ as the controller must make relevant notifications, it will ensure that any of its processors inform it of any data breach identified immediately the processor discovers it.

## 13. Data Protection Impact Assessments ("DPIA's")

Also known as a privacy impact assessment, a DPIA is a tool which can enable AKJ to identify the most effective way of complying with data protection obligations and protect customers' data. It is a privacy related assessment of how privacy can be affected by certain actions.

**When is it required?**

AKJ would be required to carry out an DPIA:

- when using new technologies: and/or
- when processing is likely to result in a high risk to the rights/freedoms of individuals

AKJ will undertake a DPIA when processing of data is:

- systematic and extensive
- large scale and related to criminal convictions or offences
- and large scale systematic monitoring of public areas.

**What would AKJ include in a DPIA?**

- A description of data processing & an explanation of the purpose & the rationale behind this processing.
- An assessment of how necessary the data processing is & also whether the processing is proportionate to the purpose.
- A risk consideration, detailing any risks to data subjects that the processing may entail.
- An outline of what measures are in place to reduce risk, including security procedures and technology used.
- A DPIA can apply to multiple projects within AKJ so it may not be necessary to start a new one for every project providing the specific data privacy related issues are covered in the existing DPIA.

This requirement to complete a DPIA is not considered to be applicable to AKJ, given the nature of AKJ's business and the fact that there are not likely to be any circumstances where AKJ could be processing data that could result in a high risk to individuals which want warrant the need to conduct such an assessment beforehand.

## 14. Privacy Notices

AKJ will provide such data privacy notice on its website so it is available to all visitors to the website. It will also provide such notice to all customers and potential customers when it starts to collect any Personal Data.

AKJ's notice(s) will include:

- what information AKJ hold that constitutes Personal Data;
- what AKJ do with the Personal Data we process;
- whether AKJ are collecting the information or getting from a 3rd party;
- whether AKH are creating derived or inferred data about people, e.g. by profiling them;
- whether AKJ will be likely to do other things with it in the future – e.g. undertaking large scale analysis of data;
- the lawful bases being used for processing categories of data;
- where consent is being requested, a clear and transparent positive opt-in for the subject;
- who such data might be shared with

## 15. Data protection by design and default

**Privacy by design** is an approach to projects that promotes privacy and data protection compliance from the start, and AKJ believes in this approach. AKJ believes it should ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example, when:

- building new IT systems for storing or accessing personal data;
- developing policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

AKJ will strive to ensure that protecting data and ensuring that employees always think about the protection of data in everything they do becomes part of daily life at AKJ and that its default position is one of awareness and compliance with the applicable regulations.

## 16. Data protection queries

All queries to do with data protection related issues should be addressed to the Compliance Department at AKJ at compliance@akj.com.