1. Baggrund

Politikken tager blandt andet sigte på at sikre;

- at Accunia overholder datasikkerhedsreglerne (GDPR)
- at fortrolige oplysninger ikke videregives uberettiget, samt
- at der er offentligt tilgængelige retningslinjer for, i hvilket omfang oplysninger videregives, jf. lov om fondsmæglerselskaber, kapitel 12.

2. GDPR

I Bilag A forefindes Accunias forretningsgang for overholdelse af GDPR. Generel information vedrørende GDPR forefindes på www.accunia.com.

3. Videregivelse af oplysninger

Ingen medarbejdere må uberettiget videregive eller udnytte fortrolige oplysninger.

Ingen medarbejdere må uberettiget videregive eller udnytte fortrolige oplysninger, som de under udøvelsen af deres hverv er blevet bekendt med, jf. lov om fondsmæglerselskaber §118.

Forbuddet gælder specielt oplysninger om en kunde til brug for markedsføring eller rådgivning.

Forbuddet gælder ikke, hvis videregivelsen sker til ATP m.fl. til brug for varetagelse af administrative opgaver, jf. §115, stk. 2, eller hvis kunden skriftligt har godkendt videregivelsen.

Den kundeansvarlige skal opbevare bekræftelsen i kundens elektroniske kundemappe.

4. Offentlig tilgængelighed

Nærværende politik skal sammen med Accunias almindelige forretningsbetingelser udleveres til eventuelt interesserede, jf. lov om fondsmæglerselskaber §119.

5. Overtrædelser af GDPR

Ved overtrædelser – eller mistanke om overtrædelse - af GDPR skal Chief Compliance Officer og direktionen underrettes uden unødigt ophold. Herefter træffes beslutning om evt. indberetning til Datatilsynet

6. Kontrol

De kundeansvarlige skal kontrollere, at der forefindes skriftlige godkendelser eller instruktioner fra kunden i de tilfælde, hvor det er nødvendigt.

7. Opdatering af politik

Denne politik gennemgås som minimum årligt med henblik på opdatering.

Således vedtaget på bestyrelsesmødet, den 19. august 2024

Peter Aandahl	Jørgen Clausen	Carsten Gomard
NJens Nødskov	Allan Gross-Nielsen	Henrik Hoffmann

Tiltrådt af direktionen

Henrik Nordby	Jacob Jensen

Bilag A – Procedure regarding GDPR

Overview

This procedure describes Accunia's procedures in order to comply with the General Data Protection Regulation (GDPR).

The following section covers an overview of the definitions of the regulatory area, whereas the following sections cover the following issues:

- Data processing in Accunia, data included and why we do it
- The right of access by the client
- The right to rectification
- The right to erasure (right to be forgotten)
- The right to restriction of processing (marketing)
- The right to data portability (to have one's data transferred to a third party)

Accunia is a financial services group and is as such obliged to process data from its clients in compliance with the Danish financial legislation and EU legislation with direct application in the member states.

In case of a discrepancy between GDPR and Financial legislation, the latter has precedence.

Definitions

The Data controller (dataansvarlige) of Accunia is the Chief Compliance Officer.

Data processors of Accunia are: The Chief Operating Officer (Chief Data Processor) and designated members of the administration team appointed by the Chief Data Processor.

Personal data are divided into normal personal data and sensitive personal data:

1. Sensitive personal data

   Data concerning race, ethnicity, political orientation, religious or philosophical orientation, union membership, biometric data which give unique identification, health information, sexual orientation/preferences, are illegal to process.

2. Normal personal data

   Social problems, other private issues, economy, tax, debt, days of absence due to illness, job related issues, family issues, home, car, examinations, applications, CVs, date where one started working, job description, field of work, work phone, name, address, date of birth etc.

Criminal convictions and offences are in a zone between the two areas.

Accunia does only process Normal personal data.

Data processing in Accunia, data included, why we to it, and where/how it is stored.

Accunia have several personal data related obligations due to Danish and EU financial legislation.

1. KYC/AML

   In connection with the start-up of a client relationship the Danish Anti Money Laundering and Corruption Law set up requirements for documention regarding a client (legitimation etc) and the client's funds. This information is stored in Accunia's IT system.

   Accunia does not process sensitive personal data in connection with this process.

2. Sutability test and continuous follow-up and reporting

   In connection with the customer relationship, Accunia will regularily have meetings or phone/email correspondence with the client. This information is store in Accunia's IT system

   Accunia does not process sensitive personal data in connection with this process. It a client, a third party, or Accunia inadvertedly causes Accunia to come into possession of sensitive personal data the Data Controller will be notified and the data deleted irrevsibly from Accunias systems.

3. Trading and trade reporting

   In connection with client trades, Accunia, in order to, execute the deal might need to transfer personal data to third parties. These will be financial institutions or Bloomberg.

   In connection with trading, Accunia is required due to financial legislation to report the trade to the Danish FSA. This is done via Bloomberg RHUB (Bloomberg ARM) which is cleared with the Danish FSA as a trade reporting mechanism.

Accunia stores information about clients as follows:

Personal data type	**Legislation**	**IT System**	**Deletion**
Name	FSA, MF, KYC, AML	PM, BB, SF	10y after leaving
Client number	MF	PM	10y after leaving
Personal identity number (CPR etc.)	FSA, MF, KYC, AML	PM, BB, SF	10y after leaving
Address, telephone number, e-mail	FSA, MF, KYC, AML	PM, SF	10y after leaving
Bank account no.	FSA, MF, KYC, AML	PM	10y after leaving
Bank depository no.	FSA, MF, KYC, AML	PM	10y after leaving
Voice recording	MF	VR	10y

AML (Anti Money Laundering). BB (Bloomberg ARM/RHUB), FSA (Finanstilsynet), KYC (Know Your Client), MF (MiFID II), PM (Portman), SF (Sales Force), VR (Voice recording system)

Clients' right to access

All Accunia clients have the right to get a copy of the data on the client in Accunia's IT system.

In case of a request the Data Controller is informed, and the data collection is collected under supervision of the Chief Data Processor.

The client have to receive copy of the data latest a month after request.

Collection is done as follows:

Data type	**Responsible**	**System**	**Output**
Personal data	Administration	Portman	Excel with static data, holdings and transactions
Mails	Client executive	Outlook Sales Force	Copy of all mails received and send to client
Minutes	Administration	Client folder Sales force	Copy of minutes in PDF format.
Voice recording	Administration (via Lisberg Dataservice)		Copy of Voice recording as mpg file
Passport, social security card etc.	Administration	Client folder	Copy
Agreements etc.	Administration	Client folder	Copy in PDF format.
Instructions and power of attorney	Administration	Client folder	Copy in PDF format.

When all collection is finalised, the Chief Data Processor send all documents etc. to client on an USB memory stick.

Clients' right to rectification

If a Client either in connection with the process mentioned in section 1.4 or by other means believes that Accunia's data are not correct, the client must notify Accunia by writing to either the CEO, the COO or the Chief Compliance Officer.

When one of the above receives a rectification request, it will be added to Accunia's GDPR list of requests, and the three officers mentioned above will be notified. The COO will prepare a report on the request, and the group will approve the decision on the matter. The Data controller will in case of different opions be ultimately responsible.

The maximum time from a request is received to the answer to the client is 1 month. Only in expectional cases this limit can be extended, and only after written approval from the Data Controller. The legislation has a final maximum time frame of 3 months.

The Data Controller and the Chief Data Processor keep a list of rectification requests with information of the data rectified.

Clients' right to erasure

A prospective client, a currently client and a former client can request the right of having all of its data deleted.

Prospective client	Present client	Former client
Data regarding prospective clients who have not made transactions nor been advised by Accunia can normally be deleted with immediate effect.	Data and activities regarding present clients are subject to financial legislation. If a request to delete data is received, the client will cease to be a present client, and become a former client (see next box)	Data regarding former clients are subject to financial legislation. Data has to be stored as mentioned under 1.3. Accunia will delete all data not subject to financial legislation with immediate effect.

The Chief Data Processor will inform the client about Accunia's regulatory ability to erase data.

The Data Controller and the Chief Data Processor keep a list of rectification requests with information of the data rectified.

Clients' right to restriction of processing

A client has the right to request the restriction of using the client's data for marketing purposes.

The Chief Data Processor and the Sales team keep a list of clients with marketing restriction.

Clients' right to data portability

A client has the right to request that its data be delivered to a third party.

Upon request, the Chief Data Processor transfer the following data in written agreement (eg. email) with the client and the third party.

Transferrable data are all data stored in Accunia's Portman system.