PERSONAL DATA POLICY

FOR

AXCEL MANAGEMENT A/S
(THE "**MANAGER**")

Contents

1. Background and purpose

1.1 This Personal Data policy sets out rules and procedures to ensure that the Manager is compliant with the regulation on handling personal data, set out in the General Data Protection Regulation (the "**GDPR**"), Regulation (EU) 2016/679, the Danish Personal Data legislation (Persondataloven), Regulation no. 429 of 31/05/2000 and the Danish Data Protection legislation (Databeskyttelsesloven), Regulation no. 502 of 23/05/2018.

1.2 The purpose of this policy is to describe how personal data is collected, stored, and processed, to ensure that all personal data is handled in accordance with the relevant legislation. The Manager has adopted measures on a risk-based approach that corresponds to the level of risk of the personal data being processed.

1.3 The Manager collects, handles, and stores personal data from four groups of persons:

- Employees (Section 6)
- Investors (Section 7)
- Network (Section 8)
- Applicants (Section 9)

All processes where the Manager receives personal data have been identified, and for each process, the lawful basis for processing the data has been determined. Section 4 below can be used as a guideline on when personal data can be stored and how it should be handled.

1.4 In section 9, the policy also deals with when and under which conditions we are allowed to transfer personal data to external parties.

2. Definitions

2.1 Capitalized words shall have the meaning as described in the list of definitions as approved from time to time by the Board of Directors. References to other policies and procedures are also capitalized.

3. Roles and responsibilities

3.1 The Board of Directors has the overall responsibility that the Manager is compliant with GDPR. Management is responsible for implementing the policy in separate privacy policies as listed in section 1.3. The Compliance Officer is responsible for communicating the policies, assuring adequate training and compliance.

3.2 All employees at Axcel shall adhere to this policy at any time when processing personal data.

3.3 The Finance department is responsible for handling personal data regarding Employees and Investors. The Administration department is responsible for handling personal data processed in cv@axcel.dk, the CV section in Admincontrol and in CRM.

4. What is personal data

4.1 Personal data is all kinds of information that directly or indirectly can be related to a physical person. This includes, but is not limited to, name, personal ID number, email, address and phone number. This also includes other kinds of identification numbers, encrypted data, and different types of electronic identities such as IP-numbers, if they can be used to identify a physical person. Some personal data may be especially sensitive such as certain information on health, sexual orientation etc. It is the Manager's policy not to retrieve and store sensitive personal data unless there is a legal obligation to do so.

5. Handling of personal data

5.1 The Manager and the employees processing personal data must have a lawful basis to do so. The lawful basis may vary for each process where we receive personal data, but can in general be grouped into the following four categories:

- **Based on consent** – e.g. when applicants send a CV and accept storage
- **Contractual basis** – e.g. to fulfil an employment contract
- **Legal obligation** – e.g. to comply with KYC requirements
- **Legitimate interest** – e.g. registration in CRM, as it is deemed to be beneficial to both the Manager and the data subject

5.2 Personal data can be processed on multiple lawful basis. If personal data e.g. is being processed both on the basis of a legal obligation and on consent, it may still be processed, even though the consent is withdrawn. In the following sections 5-8 the lawful basis for handling personal information for Employees, Investors, Network and Applicants are described in more detail.

5.3 Any sensitive and/or confidential personal data may not be sent by email unless encrypted.

5.4 Pictures of persons that are merely presenting an atmosphere and/or surroundings, and not primarily the person, may be used without a specific consent. If a specific consent is required, and Axcel may want to use the picture on an ongoing basis, it should be considered to pay a fee to the person in the picture.

5.5 Access to personal data shall be restricted to relevant employees.

6. Data on employees

6.1 Employee data includes information used by HR such as name and address, but also pictures, information on health and personal ID. All employees shall have access to

name and addresses, whereas other personal data shall be contained in the HR- or Finance department. When relevant, personal IDs may also be handled by the receptionist. The employees shall at all times have access to the most recent Privacy Policy for Employees.

6.2 HR

Information regarding the employee's name, address, contact information, salary and bank account is stored as the information is necessary to fulfil the employment contract. Handling of this data is therefore allowed on a contractual basis. Access to the personal data shall be restricted to the Finance department. Once the employee becomes a former employee and there is no longer a lawful basis to continue to store the information, the personal data shall be deleted. Recruitment letters, dismissal letters, cases of expulsions and the like may be stored if there is a legal basis usually being 5 years, following the limitation period (Forældelsesfrist). Payroll documentation can be stored as long as there is legal requirement, usually for 5 years plus the current calendar year to comply with the relevant accounting documentation requirements.

6.3 Website

The employees of the Manager may have their name, picture, position and email published on the website. Pictures may only be posted in public forums, publications and the like based on specific consent, which shall be collected from all employees, except for the Board of Directors and the Partners of the Manager.

6.4 Health

In the event that an employee is sick, the Manager may store personal data regarding the employee's health. This is classified as sensitive personal data, and shall therefore be treated accordingly. Handling of health data takes place on a legal obligation to document the employee's illness.

6.5 Bookings

The receptionists of the Manager may assist the rest of the employees with booking flights, hotels, travel agents etc. To provide the necessary information, the receptionists need access to ID-copies, personal ID-number, reward numbers, address, name and contact information. Handling and disclosure of the above mentioned information shall only take place, when the employee has given consent.

6.6 Clean-up procedures for employees

Finance shall perform an annual clean-up procedure in December of the employee- and HR-folders (noting, that any general data of employees stored in CRM is deemed allowed as also described in Axcel's privacy policies, as they will be part of the Axcel Network upon termination of employment, unless requested otherwise). Deletion of employee data should take place 5 years after termination of employment. The Finance department shall, based on an employee register they keep, check if 5 years have passed since the termination of employment for any former employee. If 5 years

have passed, all personal data in the employee / HR folder must be deleted, unless there are necessary reasons, such as legal claims.

7. Data on investors

7.1 Data on investors include normal contact details and specific information including personal ID used in the KYC process. All employees of Axcel shall have access to normal contact details and Axcel may store this information in its CRM system as Axcel and the investor have a legitimate interest herein.

7.2 KYC

All investors must provide KYC (Know Your Customer) documentation, as the Manager is required to perform measures to prevent money laundering and financing of terrorism. This means, that the manager is required to collect, process and store personal data from the investors based on a legal obligation. The investors may be requested to deliver personal data such as ID-copies, address, utility bills, name and contact information. The information is stored according to the relevant KYC/AML regulation. Access to the information is restricted solely to the Finance department and Compliance. KYC information received by email shall be stored in the designated KYC folder, and the email containing the personal data shall be deleted permanently. KYC documents may be stored for up to five years after the resolution of the fund.

7.3 Clean-up procedures for investors

Finance shall perform an annual clean-up procedure in December of the KYC folders (noting, that any general data as listed in section 7.1 on investors stored in CRM is deemed allowed as also described in Axcel's privacy policies). Deletion of investor data should take place 7 years after the resolution of the fund. To check, if any data is to be deleted, the Finance department shall extract a list from CRM once a fund reaches the seventh year anniversary from its liquidation. If an investor has invested in subsequent funds, the data cannot be deleted. If an investor has not invested in subsequent funds, and has not been investor in any Axcel fund for the past 5 years, only the personal data in the KYC folder must be deleted. This includes Passport copies, utility bills, and other personal information.

The Finance department is responsible for checking if any fund has reached a seven year anniversary from its resolution, and, if needed, that this procedure is performed by end of December.

8. Data on persons in Axcel's Network

8.1 Part of Axcel's business is maintaining a network which amongst others includes normal business contacts, and other persons with a connection to Axcel.

8.2 CRM

Persons with a close or continuous relationship with the Manager may be stored in a CRM system. The data stored includes e.g. name, email, phone number, occupation

and address. The purpose of the CRM system is to create a shared database restricted to the employees of the Manager to easily access contact information. It is a legitimate interest of the Manager, that its employees are able to reach out to the persons registered in the CRM system with business opportunities etc. The registration in the CRM system has been assessed as being beneficial to both the employees of the Manager and the data subjects. Should the data subject object to the registration, then any data regarding the data subject shall be deleted from the CRM system.

8.3 Special purpose personal data

The Manager may store data required to make travel arrangements, such as a copy of (or information from) passport and/or flight reward numbers and data required to pay out a consultant fee. Special purpose personal data is stored by Administration and processed based on consent. Administration should ensure that such data is deleted two years after the last use, or an earlier date should the data subject request this.

8.4 Newsletters

The Manager may send out a newsletter by email containing news, updates or the like about any events related to the Manager. All data subjects receiving the newsletter shall be made aware of how the Manager handles and stores their personal data. To send out the newsletter, personal data such as email, name and occupation may be stored and handled.

8.5 Events

The Manager may host events where the name, email and occupation of the invited guests are required to send out the invitation. It is a legitimate interest of the Manager that it can invite persons with a close or continuous relationship with the Manager to relevant events, which also are deemed to be beneficial to the data subject. Should the data subject no longer wish to receive invites to events from the Manager, then the Manager may no longer send out event invites to the data subject.

Pictures

In connection with events, pictures may be taken, to be used for marketing purposes, newsletters or the like. Axcel networking events are generally events, where several of the persons participating have a prominent role, function or employment. It is therefore generally deemed in the interest of both the data subject and the Manager to have the picture taken and subsequently presented in relevant media.

In order to use a picture based on legitimate interest, an overall assessment must be made for each picture. It must be assessed, whether the data subject may feel exhibited, exploited or violated by the use of the picture. If this is not the case, then it should be in the legitimate interest of the Manager to use the picture.

Based on the guidance from the Danish Data Protection Agency as of 26th September 2019, it shall no longer be distinguished between portrait pictures and situational pictures. The assessment shall therefore be made using common sense evaluating criteria such as the work title of the person, how the person is portraited on the picture and the specific situation. If there is doubt to whether a person may feel exhibited, exploited or violated by the use of the picture, the Manager shall obtain specific consent from the relevant person.

The Manager shall always inform the invited guests to such events of its Privacy Policy, which can be done by including a link to the Managers Privacy Policy in the invite.

8.6 Management-Incentive-Program

For the portfolio companies administered by the Manager, there may be an incentive program in place for the management in each portfolio company. This contains personal data such as name, address, contact information, salary and bank account number. This personal data is required to fulfill the employment contract of the incentive agreement with the data subject. The handling of data can therefore take place on a contractual basis.

8.7 Kanvas

The Manager may receive personal data when looking into potential portfolio companies. The personal data received in this process includes employee names, addresses, contact information and salary. The data is stored in the designated Kanvas folder, and/or in an online data room administered by the seller or their advisors. Before being granted access to the personal data, it is customary that the Manager enters into a Non-Disclosure Agreement. In this agreement the Manager is granted the access to the personal data by the seller. It is customary, that the data room is closed after the process is terminated, why no annual clean-up procedure is in place for this type of personal data.

8.8 Clean-up procedures for network

Administration shall perform an annual clean-up procedure in December of the special purpose personal data (noting, that any general data as listed in section 8.2, 8.4 and 8.5, and stored in CRM or relevant media is deemed allowed as also described in Axcel's privacy policies).

Deletion of special purpose personal data, as described in section 8.4, should take place annually in December. Administration much check internally if data has been unused for more than 2 years. If more than 2 years has passed, Administration must determine if renewal of consent is relevant, or if the special purpose personal data must be deleted. If renewed consent is not received, the personal data must be deleted.

The Finance department is responsible for reminding, and, if needed, that this procedure is performed by end of December.

9. Applicants

9.1 Data on applicants include data on existing and potential candidates for management in portfolio companies, and furthermore applicants for job openings in Axcel and any affiliate hereof or any potential portfolio company.

9.2 Recruitment

The Manager receives CV's from applicants unsolicited or in connection with a specific job posting. A CV received may be stored for up to 5 years if the applicant in writing has asked Axcel to store the CV and the applicant subsequently has been informed of our privacy policy for applicants or in writing has provided consent after being informed of our privacy policy for applicants. In other cases, the CV cannot be stored, unless the CV is received in connection with a specific job posting. In this case a CV may be stored for up to 6 months unless it is known at an earlier time, that the candidate will not be offered the job.

After the allowed storage period, the CV shall be delete permanently, unless consent is renewed.

A CV can be received in various ways, where the most common is by email. When a CV is received by email, the CV shall be forwarded to cv@axcel.dk or sent directly hereto. Name, email address, phone number, date of obtaining the CV (in the CRM field 'CV in Axcels database') and candidate attributes (eg industry strengths) shall be stored in CRM and the CV, evidence of adherence to this Personal Data Policy and other relevant material shall be stored in Admincontrol with no option to download, where all relevant employees will be able to access it. The email(s) in the employees mailbox containing the CV shall be deleted permanently.

CV's for specific job offerings shall be stored in a new folder designated to this while other CV's shall be stored in a general (or in limited cases in an industry specific folder noting that CV's should preferably be stored in the general folder and not industry specific folders as general attributes for the person instead should be stored in CRM which allows for better search options). A subfolder for each person shall be created where the CV and shall be stored.

The email containing the CV shall not under any circumstances be shared or forwarded, except to cv@axcel.dk. If the CV shall be shared with a colleague who is involved in the recruitment process, access to the folder in Admincontrol containing the CV's can be granted to the colleague. This procedure is also to be followed if shared with colleagues in portfolio companies.

The relevant employee of the Manager receiving the CV shall initially be responsible for informing the applicant of our Privacy Policy for Applicants, collecting the ask for

storage of the CV or consent from the applicant and uploading the CV to Admincontrol. The responsibility may be delegated to Administration by forwarding the CV to cv@axcel.dk. The Administration manages CRM, cv@axcel.dk and the CV folders in Admincontrol.

9.3 Clean-up procedures for applicants

Administration shall perform an annual clean-up procedure in December of the CV folders (noting, that any general data as listed in section 9.2 on applicants stored in CRM is deemed allowed as also described in Axcel's privacy policies). Renewal of consent shall be requested for all CV's that have been stored for more than 4 years at the time of the clean-up procedure and where Axcel finds it relevant to continue to store the CV. To check for relevance the Administration shall extract a list from CRM, share the list internally at Axcel and request feedback. If storing is still relevant, Administration shall as ask the applicant for permission to continue to store the CV. If acceptance is received, Administration should store the acceptance in the applicants cv folder and update the CRM field "CV in Axcels database" field. If acceptance is not received by the applicant, the CV folder for this applicant must be deleted.

The clean-up procedure for specific job offerings shall be initiated once the candidate for the job has been found and no later than six months after the search has started. Before deleting the CV. Administration shall consult with the relevant persons at Axcel responsible for the job search on which CVs that are relevant to keep, and ensure that Axcel has obtain approval by the applicant to store the CV.

The Finance department is responsible for reminding, and if needed checking, that this procedure is performed by end of December.

9.4 References

An important part of Axcel's business is to match the right candidates with the right job. Obtaining references is crucial part of this process. We therefore communicate in our privacy policy for Applicants that we observe the right to contact references provided by the applicant during the recruitment process. Before obtaining references not provided by the applicant regarding a specific job, consent from the applicant is required.

10. General clean-up procedure for all employees

10.1 All employees at Axcel shall erase personal data in e-mails, on an ongoing basis in accordance with this policy. The ongoing clean-up is performed using common sense and by being diligent towards minimizing and deleting personal data. Ongoing clean-up can be performed as described in 10.2 and 10.3. In addition to this, each employee shall perform an annual procedure in December, reviewing their inbox and personal files for personal data to ensure erasure and data minimization.

10.2 E-mail annual clean-up

When reviewing their e-mails in connection with the annual clean-up procedure, each employee must use common sense for which personal data they could have received. They employee delete it from their e-mail entirely, which also includes the "Deleted" folder. When reviewing their e-mail the employees must at least search for the following key words in English and Swedish or Danish and delete any emails with personal information:

- CV, Curriculum Vitae, C.V.
- Passport, drivers license, health insurance, utility bill
- CPR, personal identification number

10.3 Annual clean-up of documents stored in Sharepoint

Each employee should review their personal folders on Sharepoint in connection with the annual clean-up procedure using common sense for which personal data they could have stored. The employee must search for the same keywords as mentioned in 10.2, and either delete the personal information, or store it in a secure location, depending on the type of personal data, in accordance with this Personal Data Policy. The folders which must at least be checked are:

- Desktop
- Documents
- Downloads
- Personal OneDrive

Once personal files have been deleted, remember to also empty the "Recycle Bin".

10.4 The Finance department is responsible for reminding, and if needed checking, that this procedure is performed by end of December.

11. Disclosure of personal data

11.1 The Manager uses a range of service- and IT-providers, where personal data is stored and administered.

11.2 When any employee of the Manager shares personal data on his or hers own behalf to a service provider, it is not necessary to enter into a data processor agreement, as it is the employees own decision to share his or hers own personal data.

11.3 Some systems are cloud solutions or installed by the vendor, which means the Manager passes on personal information to the vendor. In these cases, the supplier is the Manager's data processor and handles the information on behalf of and according to

the Manager's instructions. Therefore, when personal data is shared from the Manager to a provider on behalf of the data subject, it is necessary to enter into a data processor agreement with the provider.

In accordance with Article 28(3) of the GDPR the data processing agreements must govern the following matters:

- Determine the subject and duration of the processing
- Determine the nature and purpose of the processing
- Determine the types of personal data as well as the categories of data subjects
- Determine the obligations and rights of the data controller.
- That the data processor may only process personal data on the instructions of the data controller and ensure that the persons who process the personal data have committed to confidentiality or are subject to other appropriate statutory confidentiality obligations
- That the data processor deletes or returns personal data at the instruction of the data controller
- That the data processor ensures that appropriate security measures are taken
- Whether the data processor can make use of sub-processors.

11.4 Once per calendar year the Finance department shall check the data processors' compliance with the data processing agreement. The check shall be performed by reviewing an audit or ISO reports from the data processor provided that the reports can be used to confirm adherence or if not, a confirmation from the data processor confirming adherence.If risks or breaches are identified, the monitoring can occur on a more frequent basis. The compliance monitoring should demonstrate that sufficient assurance has been established for the personal data concerned and that this is done by using appropriate technical and organisational measures.

11.5 In exit processes, Axcel shall ensure that personal data is handled correctly and that no personal data is disclosed if there is no lawful basis. On areas where it is difficult to conclude whether there is a legal basis for sharing the personal data, Axcel shall obtain appropriate legal counseling.

12. The rights of the data subject

12.1 The following is a list of the rights of the data subject. At all times, the rights of the data subject shall follow the current legislation:

12.1.1 <u>Necessary handling of personal data and handling based on consent</u>

Personal data processing, necessary to fulfill an agreement with the data subject or to fulfill a legal obligation, is permitted without consent. However, if the Manager collects and handles personal information for another purpose, the Manager will have to obtain consent from the data subject.

12.1.2 Withdrawal of consent

The data subject may at any time choose to withdraw personal data which is stored based on consent by contacting the Head of Finance and Compliance at the Manager. If the data subject revokes the consent, the personal information shall be deleted, and the processing that previously was covered by the consent shall be discontinued.

12.1.3 How to request information about the personal data which has been stored and processed

The data subject may request information about the personal data which has been stored and processed by the Manager. The Head of Finance and Compliance at the Manager can be contacted with these requests.

12.1.4 Right to control the personal data

The data subject is entitled to request, that the information about the data subject shall be deleted, supplemented or corrected. The data subject also has the right to request that the processing of the personal information is limited to specific purposes and for example cannot be used directly for advertising or so-called profiling.

13. Review of the Personal Data policy and procedures

13.1 In addition to an annual review, the Personal Data policy and procedures shall be reviewed where:

(a) Internal or external events indicate that an additional review is required, e.g. if the relevant legislation is updated; or

(b) Material changes are made to the types of data being handled or the purposes of handling data, if different than described in this policy.

14. Amendments, approval and reporting

14.1.1 The Board of Directors shall on an ongoing basis assess and review the Personal Data policy.

14.1.2 The Board of Directors shall prepare Privacy Policies in accordance with our obligation to inform the data subject and reflecting the principles in this Policy.

14.1.3 The Board of Directors authorizes Management to approve amendments and adjustments to the Privacy Policies.

14.2 Non-adherence to this policy shall be reported by any and all employees of the Manager within a reasonable period of time to Management and the Compliance Officer.

14.3 In the event that corrective actions are not taken, Management or the Compliance Officer shall ensure that the Board of Directors are informed directly.

14.4 In the event that a data subject thinks, that the Manager violates the applicable regulation on personal data protection, the data subject may contact the Danish Data Protection Agency (For more information see www.datatilsynet.dk).

14.5 In the event that a breach/incident takes place, as defined in the GDPR, the Comliance Officer must notify the Danish Data protection Agency and the data subject within 72 hours from becoming aware of it. If the notification is not made within 72 hours, it shall be accompanied by reasons for the delay. If the breach is unlikely to result in a risk to the rights and freedoms of natural persons, a notification is not required.

15. Approval

15.1 This policy was latest approved by the Board of Directors on the 25 April 2022.

16. Approval history

Version:	Effective from:	Changes:
0	24 April 2018	Draft policy
1	28 August 2018	Policy approved
2	11 April 2019	Roles and responsibilities, withdrawal of consent and storing of CV's.
2.1	19 November 2019	Updated treatment of pictures
2.2	31 August 2020	Updated several descriptions and guidelines including clean-up procedures
2.3	25 April 2022	Notification to the data subject