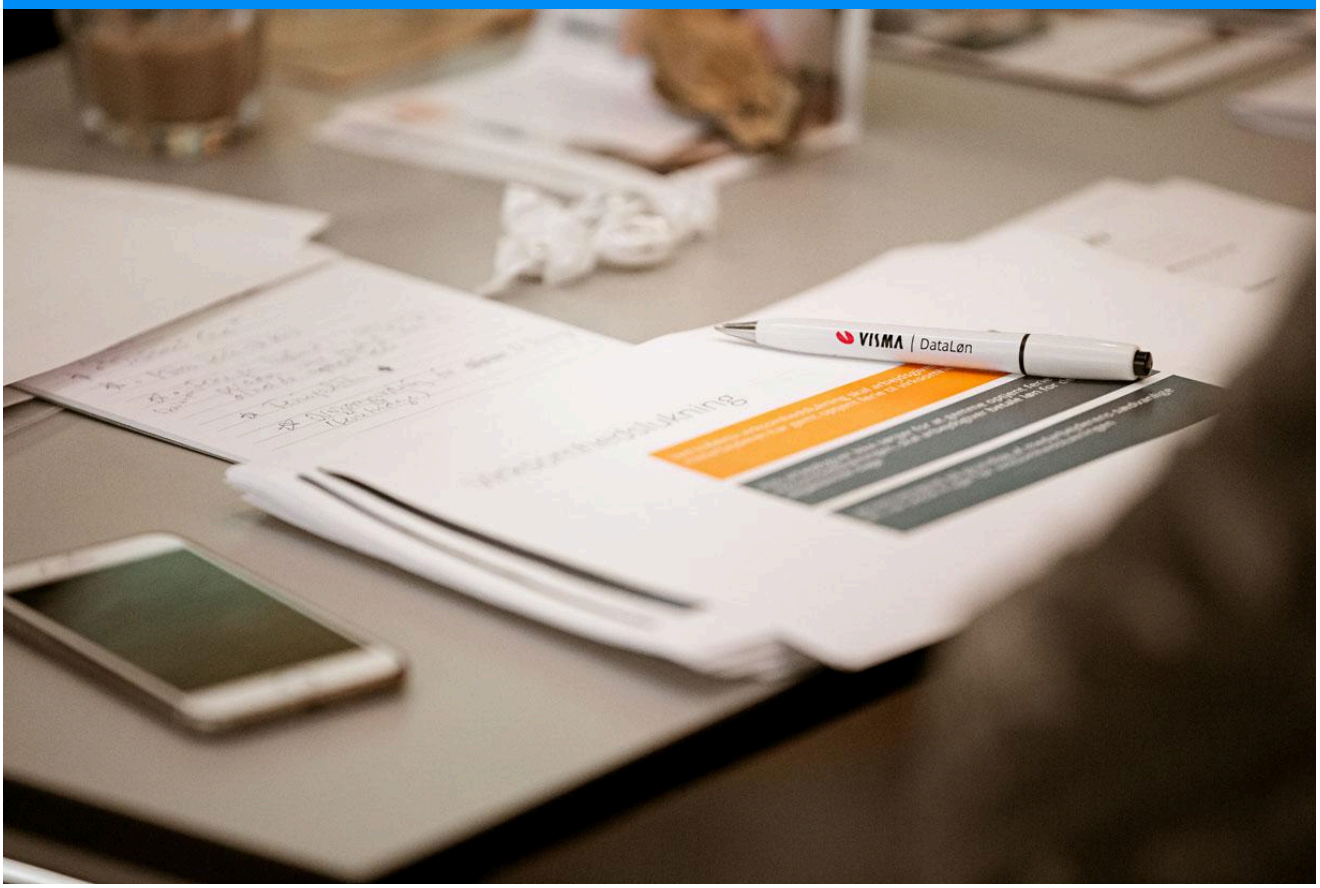
Terms and conditions for DataLøn



Effective November 1, 2024

DataLøn

Table of Contents

1. What is Dataløn?

Dataløn is a payroll system. The core of Dataløn is a standard IT solution which, based on the Customer's reports to Visma Dataløn, conducts salary processing for the Customer. This includes:

- calculating the Employees' salaries;
- making all calculations and reports to arrange for money transfers to SKAT, ATP (Labour market pension), holliday funds, maternity funds, pension funds, etc. on behalf of the Customer;
- reporting statistics to employers' associations and Statistics Denmark on behalf on the Customer;
- sending payslips to the Employees' digital mailbox;
- saving the Customer's salary documents in an electronic archive for 5 years after the end of the year in which the salary document is produced;
- start-up assistance and help creating the Customer and the Employees; and
- support and consultancy services over the phone and online from Visma Dataløn's payroll consultants whenever the Customer needs help.

Visma DataLøn exchanges data electronically with third parties and makes changes to registered master information at the request of third parties, e.g. TAX and pension companies. Affected customers are informed by a third party or by Visma DataLøn.

Depending on the subscription type, the Customer can get legal advice on employment law, and templates for personnel administration etc. The material is updated on an ongoing basis.

A more detailed description of DataLøn, including the various types of subscriptions and associated product content, is available on dataløn.dk.

Visma DataLøn does not develop or customise DataLøn to the Customer's specific needs or requests.

2. Definitions

2.1. Visma DataLøn

Visma DataLøn og ProLøn A/S, Company registration (CVR) no. 48 11 77 16 is the company providing DataLøn.

2.2. Agreement

These terms and conditions for DataLøn, including appendices and the current prices on dataløn.dk. The Agreement constitutes the overall contractual basis between Visma DataLøn and the Customer in relation to DataLøn.

2.3. Banking day

Every day, with the exception of Saturdays, Sundays, and public holidays, the Friday following Ascension Day, 5 June and 24 and 31 December.

2.4. Payment basis

The Payment basis generated in the salary processing by Visma DataLøn that forms the basis for money transfers to the Customer's employees, SKAT, ATP (Labour Market Pension), pension funds, etc.

2.5. DataLøn
Reference is made to condition 1.

2.6. dataløn.dk
The terms and condition will be available at www.dataløn.dk

2.7. Legal Consulting in DataLøn
Legal Consulting provides general and specific telephone and/or written legal advice on employment law matters based on information from the Customer.

Visma DataLøn's advisers are either lawyers or other employees who are internally trained in personnel law at Visma DataLøn.

2.8. Basic data
All data about the Customer and the Employees to be used for salary processing, delivered by the Customer to Visma DataLøn or collected by Visma DataLøn on behalf of the Customer.

2.9. The Customer
The company (employer) with which Visma DataLøn has signed this Agreement for the use of DataLøn.

2.10. Employees
Those of the Customer's employees, consultants, etc. which the Customer has registered in DataLøn (individually referred to as "Employee").

2.11. NemRefusion (Easy Reimbursement)
Public digital reporting solution for notification of sickness absence or absence due to maternity/paternity leave and requests for reimbursement of sickness or maternity/paternity leave benefits and unemployment benefits according to maternity/ paternity law.

2.12. Overførselsservice (Transfer service)
Overførselsservice is a product provided by Mastercard Payment Services Denmark A/S (Mastercard), whereby Mastercard, on behalf of the Customer, processes and forwards the Payment Basis to the Customer’s bank for the purpose of transferring money to the recipient.

2.13. Samlet Betaling (Collective Payment)
ATP administers Samlet Betaling which, on signing the Agreement, covers calculation and collection of contributions for AUB, AFU, AES, Barsel DK and Financing contributions. The contribution to the schemes in force from time to time under Samlet Betaling, will automatically be calculated on the basis of ATP contributions. Contributions for Samlet Betaling are collected on a quarterly basis.

2.14. Master Data
The personal data and other information registered for the individual employee and which is documented on the employee’s data card, including information regarding pension schemes, holiday allowance, weekday holiday allowance (SH), and elective scheme (fritvalg).

3. Money transfer

3.1. Transfer related to salary processing

Transfer of

I. funds to Employees based on the Payment Basis
II. the Customer's payment to Visma DataLøn for services pursuant to the Agreement, and
III. funds to SKAT, ATP, holiday and maternity funds, pension schemes, etc., shall be drawn on the bank account specified by the Customer to Visma DataLøn. Transfers take place via Overførselsservice.

Transfers take place in accordance with the applicable rules for Overførselsservice and for the Customer's payment account with the Customer's bank, respectively. Such regulations are of no concern to Visma DataLøn.

3.2. Transfer via Samlet Betaling

When registering for Samlet Betaling in DataLøn, the Customer gives consent for ATP to initiate payments from the Customer to ATP. Transfers to Samlet Betaling take place via Overførselsservice.

The Customer can unsubscribe from Samlet Betaling prior to the first day of the month before the last due payment date.

4. Customer obligations

4.1. Registration

Visma DataLøn has an obligation towards SKAT to ensure that the Customer is registered correctly with respect to eIndkomst (e-income) before Visma DataLøn can obtain eSkattekort (e-tax card) and submit information to eIndkomst.

The Customer authorizes Visma DataLøn to make requests about the Customer's registrations in relation to eIndkomst and if agreed update the record in the Central Business Register according to the above if it is incorrect and not up to date.

Regardless of the above, it is the Customer's responsibility and a precondition for the Customer's correct use of DataLøn that the Customer's business can be registered correctly in the Central Business Register. If this is not the case, it is considered a material breach of the Agreement.

4.2. Agreement regarding Overførselsservice

In order for the Customer to complete money transfers, see condition 3, an agreement must at all times exist between the Customer and Mastercard for the use of Overførselsservice.

4.3. Employee Master Data

The Customer is obligated to ensure that the Master Data registered by Visma DataLøn when creating or changing Employees on the basis of Basic Data from the Customer is correct at all times.

4.4. Basic Data

The Customer is responsible for delivering the Basic Data to DataLøn via entering it directly into DataLøn

4.5. Customer's IT equipment

The Customer's IT equipment must satisfy the system requirements specified at dataløn.dk.

4.6. Customer's liability
The Customer is liable for all transactions, which the Customer, the Employees or others outside Visma DataLøn have made via DataLøn, including in case of unauthorised use.

4.7. Customer storage
The Customer must store the Basic Data in accordance with legislation, including the Danish Bookkeeping Act.

4.8. Customer information
The Customer is obliged to ongoingly provide Visma DataLøn with updates to all relevant information, which the Customer has given to Visma DataLøn in connection with the commencement of the Agreement, including information about the Customer's name, address, phone number, email address, and bank account.

5. Data processing

5.1. Data controller
The Customer is the data controller and is responsible for processing the personal data, which the Customer processes and sends to Visma DataLøn for the purpose of Visma DataLøn's performance of the agreement.

5.2. Data processor
Visma DataLøn is the processor, pursuant to the General Data Protection Regulation and the Danish Act on Processing of Personal Data in force from time to time, and exclusively processes information on behalf of the data controller. Specific terms are regulated via the data processor agreement appended as Appendix 1.

6. Prices and payment

6.1. Prices
Visma Dataløn's services will be invoiced according to the current prices on dataløn.dk plus VAT.

The Customer shall not have to pay Visma DataLøn separately for the Customer's use of Overførselsservice in relation to DataLøn. Any request for payment from the Customer's bank regarding the use of the Customer's payment account is of no concern to Visma DataLøn.

6.2. Payment
The Customer's payment for services under the Agreement involves Visma DataLøn transferring the invoiced amount from the Customer's account, see condition 3.1.

7. Requesting information from the Danish Civil Registration System (CPR)

Via DataLøn, the Customer can request information about employees' names and addresses in the Civil Registration System (CPR). If the Customer uses this feature, the following conditions apply:

- The Customer may only request information from CPR about individuals to whom the Customer, on account of an agreement, will pay out salary, fees etc.l.

- The Customer's processing of the information received from CPR, must take place in accordance with the General Data Protection Regulation and the Danish Act on Processing of Personal Data as it exists from time to time.

Intentional or grossly negligent violation of the aforementioned conditions for requesting information from CPR is a punishable offense.

Visma DataLøn registers user ID, time, and civil registration number for every request for information from CPR in the Customer's name. Visma DataLøn stores this information for six months, after which it is deleted. Upon request, Visma DataLøn shall surrender the information to CPR.

8. Reimbursement requests etc.

If the Customer wishes for Visma DataLøn to report reimbursement requests on behalf of the Customer, the Customer can provide Visma DataLøn with a corporate proxy. When the Customer provides Visma DataLøn with a corporate proxy, the Customer at the same time gives consent to Visma DataLøn reporting data to NemRefusion on behalf of the Customer.

Reporting to NemRefusion is done on the following conditions:

- Information may only be reported to NemRefusion for employees who are covered by this Agreement.
- The Customer is responsible for the correctness of the data reported to Visma DataLøn for the processing of reimbursement requests. By means of error messages and receipts from NemRefusion, Visma DataLøn checks that reports are accepted in NemRefusion and ensures that any errors and omissions which NemRefusion notifies about are amended.
- Reports which are not signed ("drafts") are deleted from NemRefusion without further notice six months after the Customer's last use of the reports. Signed reports are deleted from NemRefusion 24 months after the time of signing without further notice.
- Reporting of incorrect or misleading information to be used for decisions in accordance with the Sickness Benefits Act or acts governing the right to leave of absence and unemployment benefits for maternal/paternal leave are punishable under the criminal code. The same applies to non-disclosure of information of significant importance for such decisions.
- The local authority receiving the reported information has access to the Customer's premises and workplaces for the purpose of checking salary payments etc., which constitute the basis for the calculation of sickness and maternal/paternal benefits.

9. Liability and disclaimer

9.1. Liability of the parties

Unless otherwise stated in the Agreement, the parties are liable in accordance with the general rules of Danish law.

The parties are only liable for their own services and conditions (including their sub-suppliers, other sup-pliers, and employees

Visma DataLøn therefore shall not be liable for

- the Customer's own errors or negligence, including erroneous data entering, incorrect use or abuse of DataLøn;
- whether DataLøn's functionality and content support the Customer's specific needs;
- whether the salary processing, including the Basic Data or the Payment Basis, accords with the Employees' terms of employment and/or the collective agreements which the Employees may be covered by;
- circumstances related to the Customer's bank, a DataLøn administrator with which the Customer has concluded agreement, or other suppliers of payroll administration, programmes, hardware components or other equipment, communication lines, or other supplies necessary or appropriate in order to be able to use Visma DataLøn's service, or;
- errors and actions of third-party suppliers, e.g. SKAT or digital mailbox.

9.2. Properties of templates for personnel administrative work etc. (depending on subscription type)

Visma DataLøn assumes no liability for whether a template has the required properties.

If the Customer alters a template (except for filling in standard information such as name etc.), Visma DataLøn shall no longer be liable for the relevant template.

9.3. Force majeure

Visma DataLøn is not liable for losses, including losses caused by breakdown of/missing access to IT systems or damage to data in such systems, caused by force majeure or similar conditions. Force majeure means conditions outside Visma DataLøn's reasonable control and which Visma DataLøn could not reasonably have predicted on conclusion of the Agreement, including as a result of:

- power failure or breakdown of telecommunications;
- legislative or administrative intervention;
- natural disasters, water damage, earthquake, or extreme weather conditions;
- fire;
- war or imminent war, revolution, civil unrest, sabotage, terrorism (including cyber terrorism), or explosions;
- burglary or vandalism (including computer viruses and hacking); or
- strikes, lockouts, boycott, or blockade, regardless of whether the conflict is aimed at or initiated by the parties themselves or their organisation, and irrespective of the reason for the conflict. This also applies when the conflict only affects parts of a party's organisation.

The exemption from liability applies for the duration of the force majeure event.

9.4. Limitation of liability

Visma DataLøn shall not in any case be liable for the indirect losses of the Customer or any third party, including, but not limited to, loss of production, sales, profit, goodwill, internal working hours spent, image, employees, customers, or interest.

Visma DataLøn assumes product liability according to the general rules of Danish law, whereas the limitation of liability in conditions 9 and 20 will apply in the widest possible sense permitted by Danish law.

Visma DataLøn's total liability for any single claim under this

I. agreement is limited to the amount paid by the Customer to Visma DataLøn for the 12 months prior to the time when the Customer made the claim against Visma DataLøn less
II. any other liability incurred by Visma DataLøn towards the Customer within the same 12-month period. The limitation of liability specified in this section under condition 9.4 does not, however, apply to compensation paid by Visma DataLøn in accordance with condition 20 below.

The limitations of liability in the conditions mentioned above apply to any type of claim, including the Customer's direct claims and to the Customer's claim for contribution for compensation paid by the Customer.

The limitations in this condition shall not apply if Visma DataLøn has acted intentionally or with gross negligence.

10. Defects and delays

10.1. Defects

In case of defects in DataLøn's services which are caused by Visma DataLøn, Visma DataLøn may elect to

- remedy such defect, to the extent that it is practicable and can be done without unreasonable financial consequences; or
- redeliver the performed work.

10.2. Delays

If, for reasons of which the Customer cannot be held responsible, Visma DataLøn's service is delayed, the Customer may demand that Visma DataLøn commence the delivery.

10.3. Defects and delays for which Visma Dataløn is not responsible

If Visma DataLøn is not responsible for defects or delays, Visma DataLøn, upon request by the Customer, assist with remedying or replacing against reasonable remuneration

10.4. Warranty period

Defects and delays in Visma DataLøn's services of which the Customer becomes aware or should have become aware, and which the Customer wants to invoke, must immediately be notified in writing to Visma DataLøn. If a defect or delay which the Customer discovers or should have discovered is not immediately notified in writing to Visma DataLøn, this may not be invoked at a later point in time.

10.5. Claims

Claims against Visma DataLøn as a result of defects or delays of which the Customer has given due notice, see condition 10.4, must always be made in writing and within a reasonable time and no later than six months after the expiry of the claim notification period, see condition 10.4.

11. Licence

Visma DataLøn grants the Customer a non-exclusive and non-assignable right of use for DataLøn commercially throughout the term of the Agreement, including material provided by

Visma DataLøn to the Customer under this Agreement on the conditions set out in the Agreement.

The right of use only covers the Customer's use of DataLøn for the Customer's own purposes. The Customer is entitled to engage an administrator who has acquired a right of use from Visma DataLøn to use DataLøn.

12. Intellectual property rights

Visma DataLøn has ownership, copyright and any other rights related to DataLøn, including the software, dataløn.dk, and Visma DataLøn's documentation and guidelines regarding DataLøn, with the exception of software or other material from suppliers, see condition 15.

13. Third-party rights

13.1. Infringement of third-party rights

As far as Visma DataLøn is aware, DataLøn does not infringe any third-party rights, including patents or copyrights.

13.2. Action against the customer

If a third party makes claims against the Customer asserting that DataLøn infringes third-party rights

I. the Customer must immediately notify Visma DataLøn in writing and keep Visma DataLøn updated on all matters related thereto, and
II. Visma DataLøn is, at its own expense, entitled to become a party to the case whereby Visma DataLøn can take any action on behalf of the Customer in relation to the case, including
    A. to defend or settle claims made against the Customer and
    B. engage external advisers to act on behalf of the Customer.

If any third-party rights have been infringed, Visma DataLøn must, at its own expense, provide the Customer with the right to continue to use DataLøn or bring the infringement to an end by altering or replacing Visma DataLøn's service, if practicable, and if Visma DataLøn's associated costs are proportionate to

I. the fee payable for DataLøn by the Customer or
II. the part of Visma DataLøn' service that has to be altered or replaced.

Visma DataLøn must indemnify the Customer for any amounts which, according to final court decision, the Customer is ordered to pay to the third party as a consequence of the infringement. Visma DataLøn's liability for loss shall, however, be limited as described in condition 9.

If Visma DataLøn decides not to become a party to the case, Visma DataLøn must indemnify the Customer for any legal costs which the Customer is ordered to pay to the plaintiff. Visma DataLøn's liability for loss shall, however, be limited as described in condition 9.

The provisions in condition 13 do not apply to services from suppliers, see condition 15.

14. Duty of confidentiality

Visma DataLøn shall comply with the confidentiality regulations covering the processing of personal data, cf. the data processor agreement appended as Appendix 1.

Furthermore, Visma DataLøn and Visma DataLøn's employees have a duty of confidentiality with respect to any confidential information about the Customer, trade secrets, business

associate information, and other confidential matters, with which Visma DataLøn becomes acquainted while fulfilling the terms of the Agreement.

Confidential information from the Customer may only be used and stored as part of the fulfillment of the terms of the Agreement.

15. Use of other suppliers

15.1. Visma DataLøn's sub-suppliers

Visma DataLøn may use sub-suppliers. Visma DataLøn is liable for its sub-suppliers' services in the same way as for its own services.

15.2. The Customer's sub-suppliers

At its own expense, the Customer must enter into agreements with other suppliers for the supply and installation of software, communication lines and/or other equipment that is required or appropriate to be able to use Visma DataLøn services.

16. Changes

16.1. Changes to DataLøn and dataløn.dk

Visma DataLøn is at all times and without notice entitled to make changes to DataLøn, dataløn.dk and Visma DataLøn's documentation and guidelines regarding DataLøn, including as a result of updates, renewal and maintenance.

16.2. Changes to this agreement

Visma DataLøn may change these terms and conditions for DataLøn, including the prices, at one month's written notice to the first day of any month. However, this does not apply if regulatory requirements, security considerations or similar issues necessitate shorter notice.

Visma DataLøn shall notify the customer about changes by letter or electronically, e.g. by email, inbox message or documents in E-arkiv.

17. Termination and cancellation

17.1. Termination

The Customer may terminate the agreement at one month's written notice to the first day of any month.

Visma DataLøn may terminate the agreement at three month's written notice to the first day of any month.

17.2. Cancellation

The Agreement may be canceled entirely or partially by:

- Visma DataLøn, if the Customer is in material breach of the Agreement, e.g. (i) if there is no coverage for amounts invoiced by Visma DataLøn, see condition 6, or (ii) if no agreement exists at all times between the Customer and Mastercard for the use of Overførselsservice.

- The Customer, if Visma DataLøn is in material breach of the Agreement and Visma DataLøn, after receipt of a written demand to remedy the breach, see condition 10.4, or written demand to commence delivery, see clause 10.2, has not within reasonable time remedied the breach; or

- either party, if the other party is declared bankrupt, is subject to reorganisation proceedings or a similar debt scheme unless the estate, in accordance with the regulations of the Bankruptcy Act has the right to become a party to or continue the Agreement and chooses to do so.

17.3. Outstanding services

Even when the Agreement has been terminated, it shall still be valid for obligations to be fulfilled for up to 6 months after the termination of the Agreement.

These services are provided in accordance with and on the terms of the Agreement.

If the Agreement expires due to bankruptcy, the services that are outstanding will not be executed.

18. Transfer

Neither of the parties may, without the other party's written consent, transfer its rights and obligations pursuant to the Agreement to a third party. However, Visma DataLøn has the right to transfer its rights and obligations pursuant to the Agreement to another company in the Visma group without the consent of the Customer.

19. Precedence, applicable law and venue

In case of dispute, these terms for DataLøn shall take precedence over dataløn.dk and Visma DataLøn's documentation and guidelines relating to DataLøn and the current prices on dataløn.dk.

The Agreement is subject to Danish law. Any disputes between the parties, which cannot be solved by negotiation, can be brought before the ordinary courts of law with the jurisdiction of Visma DataLøn's local court as venue.

20. Additional terms and conditions for legal advice

DataLøn customers have access to legal advice regarding Danish employment law, possibly against separate payment (depending on the type of subscription). The following terms and conditions apply when Visma DataLøn provides employment law advice as part of DataLøn.

20.1. Legal advice

Legal Consulting in Visma DataLøn provides general legal advice via telephone advice in relation to personnel administration and employment law available to the Customer.

In addition, it is possible to purchase consultancy tasks within personnel administration and employment law, which Visma DataLøn must resolve for the Customer based on the Customer's order. The task is defined in cooperation between Visma Dataløn and the customer. Visma DataLøn provides an oral or written description of the task to be performed. The description includes a description of the scope and content of the task, the estimated time consumption and the time of delivery of the task to the Customer.

Visma DataLøn's advisers are either lawyers or other employees who have received internal employment law training at Visma DataLøn.

All tasks are performed in accordance with good practice for legal counseling.

20.2. Disclaimer

In relation to liability arising from legal advice, the third section of condition 9.4 above is replaced by the following

If, as a result of the provision of legal advice, Visma DataLøn is responsible for the Customer's direct loss, Visma DataLøn's liability is limited to DKK 250,000 per task.

Appendix 1

Data processing agreement

As part of the agreement between the parties, the following Data Processing Agreement applies per article 28(3) of regulation 2016/679 (the General Data Protection Regulation) between:

Visma DataLøn og ProLøn A/S
CVR 48117716
Gærtorvet 1-5
1799 København V.
Danmark

hereinafter the “data processor”

and

the customer

hereinafter the “data controller”

each independently referred to as a “party” and jointly as the “parties”

Table of Contents

1. Preamble

1. These provisions set out the rights and obligations of the data processor when processing personal data on behalf of the data controller.

2. These provisions have been prepared for the purpose of the parties' observance of article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In connection with the delivery of the agreed service, the data processor processes personal data on behalf of the data controller in accordance with these provisions.

4. The provisions take precedence in all matters in relation to any similar provisions in other agreements between the parties.

5. Four appendices are attached to these provisions, and the appendices form an integral part of the provisions.

6. Appendix A contains detailed information about the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors the use of which has been approved by the data controller.

8. Appendix C contains the data controller's instructions as regards the data processor's processing of personal data, a description of the security measures that the data processor must as a minimum implement, and how the data processor and any sub-processors are monitored.

9. Appendix D contains provisions concerning other activities not covered by the provisions.

10. The provisions with related appendices must be stored in writing, including electronically, by both parties.

11. These provisions do not release the data processor from obligations which have been imposed on the data processor under the General Data Protection Regulation or any other legislation.

2. Rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data is made in accordance with the General Data Protection Regulation (see article 24 of the regulation), data protection provisions in other EU law or the national laws of member states and these provisions.

2. The data controller has a right and a duty to make decisions about for which purpose(s) and by which means processing of personal data may take place

3. The data controller is responsible, among other things, to ensure that there is a processing basis for the processing of personal data which the data processor is instructed to perform.

3. The data processor acts according to instructions

1. The data processor may only process personal data according to documented instructions from the data controller unless required under EU law or the national laws of member states that the data processor is subject to. These instructions must be specified in appendices A and C. Subsequent instructions may also be given by the data controller, while processing of personal data is carried out, but the instructions must always be documented and kept in writing, including electronically, together with these provisions.

2. The data processor notifies the data controller immediately if, in the data processor's opinion, an instruction is in contravention of this regulation or data protection provisions in other EU law or the national laws of the member states.

4. Confidentiality

1. The data processor may only give access to personal data that is being processed on behalf of the data controller to persons who are subject to the data processor's powers of direction, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, The list of persons granted such access must be reviewed on an ongoing basis. Based on that review, access to personal data may be barred if the access is no longer necessary, and accordingly the personal data must not longer be accessible to these persons..

2. At the request of the data controller, the data processor must be able to prove that the said persons who are subject to the data processor's powers of direction, are subject to the above duty of confidentiality.

5. Security of processing

1. Article 32 of the General Data Protection Regulation stipulates that, in view of the level of technology, costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying probability and severity for the rights and freedoms of natural persons, the data controller and processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller must assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to counter these risks. Depending on their relevance, they may include:

   a. The anonymisation and encryption of personal data

b. the ability to ensure the ongoing confidentiality, integrity, availability and robustness of processing systems and services

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of the processing.

2. According to article 32 of the Regulation, the data processor - independently of the data controller - must assess the risks to the rights of natural persons posed by the processing and implement measures to counter these risks. For the purpose of this assessment, the data controller must make the necessary information available to the data processor so as to enable the data processor to identify and assess such risks.

3. In addition, the data processor must assist the data controller with its compliance with the data controller's obligation under article 32 of the regulation, in part by making the necessary information available to the data controller concerning the technical and organisational security measures that the data processor has already implemented under article 32 of the regulation, and against invoicing all other information necessary for the data controller's compliance with its obligation under article 32 of the regulation. Terms of the data controller's control of the data processor are described in appendix C.

4. If countermeasures regarding the identified risks - in the assessment of the data controller - require implementation of measures further to those already implemented by the data processor, the data controller must specify the further measures to be implemented in appendix C.

6. Use of sub-processors

1. The data processor must meet the conditions set out in article 28(2) and (4) of the General Data Protection Regulation in order to make use of another data processor (a sub-processor).

2. Thus, the data processor may not use a sub-processor to fulfill these provisions without prior general written approval from the data controller.

3. The data processor has the data controller's general approval to use sub-processors. The data processor must inform the data controller in writing about any planned changes regarding addition or replacement of sub-processors giving at least one month's notice to the first day of any month and thus give the data controller the possibility of objecting to such changes before the use of the said sub-processor(s). The list of sub-processors that the data controller has already approved appears in appendix B.

4. When the data processor uses a sub-processor in connection with the performance of specific processing activities on behalf of the data controller, the data processor must, through an agreement or other legal document according to EU law or the national laws of member states, impose on the sub-processors the same data protection obligations as those these provisions, whereby in particular the necessary guarantees are made that the sub-processor will implement the technical and organisational measures in such a manner that the processing complies with the requirements in these provisions and the General Data Protection Regulation.

5. The data processor is therefore responsible for demanding that as a minimum the sub-processor complies with the data processor's obligations under these provisions and the General Data Protection Regulation.

6. Sub-processor agreement(s) and any later changes to them must be sent - at the data controller's request to that effect - as a copy to the data controller who thus is given the possibility to ensure that similar data protection obligations that follow from these provisions, are imposed on the sub-processor. Provisions on commercial terms not relating to the regulatory data protection aspects of the sub-processor agreement, should not be sent to the data controller.

7. If the sub-processor fails to perform its data protection obligations, the data processor remains fully responsible toward the data controller for the compliance with the sub-processor's obligations. This does not impact the rights of the data subjects appearing in the General Data Protection Regulation, in particular articles 79 and 82 of the regulation, to the data controller and the data processor, including the sub-processor.

7.1 Transfer to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations may only be made by the data processor based on documented instructions to that effect from the data controller, and must always be made in accordance with chapter V of the General Data Protection Regulation.

2. If transfer of personal data to third countries or international organisations that the data processor has not been instructed by the data controller to perform are required according to EU law or the national laws of the member states to which the data processor is subject, the data processor must inform the data controller of this legal requirement before processing, unless the said law prohibits such notification on the grounds of important public interest.

3. Without documented instructions from the data controller, within the framework of these provisions, the data processor thus cannot:

    a. transfer personal data to a data controller or a data processor in a third country or an international organisation
    b. have the processing of personal data done by a sub-processor in a third country
    c. process the personal data in a third country.

4. The data controller's instructions concerning transfer of personal data to a third country, including any basis for transfer in chapter V of the General Data Protection Regulation on which the transfer is based, must be stated in appendix C.6

5. These provisions should not be confused with the standard contract clauses as mentioned in article 46(2)(c) and (d) of the General Data Protection Regulation, and these provisions cannot form a basis for transfer of personal data as mentioned in chapter V of the General Data Protection Regulation.

8. Assistance for the data controller

1. In consideration of the nature of the processing, the data processor assists the data controller to the extent possible by means of appropriate technical and organisational measures with fulfilling the data controller's obligation to respond to

requests on the exercise of the data subjects' rights as set out in chapter III of the General Data Protection Regulation.

This means that, where possible, the data processor must assist the data controller in connection with the data controller's ensuring compliance with:

a. the duty to inform when collecting personal data from the data subject
b. the duty to inform if personal data are not collected from the data subject
c. right of access
d. right to rectification
e. right to erasure ("the right to be forgotten")
f. right to restriction of processing
g. duty to notify regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to objection
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller under provision 6.3, the data processor further assists the data controller, in consideration of the nature of the processing and the information available to the data processor, with:

   a. the data controller's duty, without undue delay and where possible by no later than 72 hours after it has been aware thereof, to report a personal data breach to the competent supervisory authority, Datatilsynet (the Danish Data Protection Agency), unless it is unlikely that the personal data breach entails a risk in relation to the rights or freedoms of natural persons

   b. the data controller's duty to inform without undue delay the data subject of a personal data security breach when the breach will likely entail a high risk to the rights and freedoms of natural persons.

   c. the data controller's duty, prior to the processing, to perform an analysis of the consequences of the intended processing activities for protection of personal data (an impact assessment)

   d. the data controller's duty to consult the competent supervisory authority, Datatilsynet before processing if a data protection impact assessment shows that the processing will lead to a high risk in the absence of measures implemented by the data controller to limit the risk.

3. In appendix C, the parties must state the required technical and organisational measures by which the data processor must assist the data controller and to which extent.

9. Communication regarding personal data breach

1. The data processor notifies the data controller without undue delay after having become aware of a personal data breach.

2. The data processor's notification to the data controller must, where possible, be made no later than 24 hours after that the data processor has become aware of the breach so that the data controller can comply with its obligation to report the

personal data breach to the competent supervisory authority, see article 33 of the General Data Protection Regulation.

3. The data processor must assist the data controller with reporting the breach to the competent supervisory authority. This means that the data processor must assist in obtaining the information below which according to article 33(3) must appear in the data controller's report of the breach to the competent supervisory authority:

    a. the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
    b. the likely consequences from the personal data breach
    c. the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. In appendix C, the parties must state the information which the data processor must obtain in connection with its assistance to the data controller in its obligation to report personal data breaches to the competent supervisory authority.

10. Erasure and return of information

1. On cessation of the services concerning processing of personal data, the data processor is obliged to erase or return all personal data having been processed on behalf of the data controller, according to agreement, unless EU law or the national laws of member states prescribe storage of the personal data.

   The data processor only undertakes to process the personal data for the purpose(s), the period and under the conditions prescribed by these rules.

11. Audits, including inspection

1. The data processor makes all information required to demonstrate the compliance with article 28 of the General Data Protection Regulation and these provisions available to the data controller and provides the possibility for and contributes to audits, including inspections made by the data controller or another auditor that has been authorised by the data controller.

2. The procedures of the data controller's audits, including inspections, with the data processor and sub-processors are specified in detail in appendices C.7. and C.8.

3. The data processor is obliged to give supervisory authorities which according to the applicable legislation have access to, in the data controller's or the data processor's facilities, or representatives acting on behalf of the supervisory authorities, access to the data processor's physical facilities against due legitimation.

12. The parties' agreement on other matters

1. The parties may agree on other provisions concerning the service about processing of personal data on e.g. liability for damages as long as these other provisions are not directly or indirectly contrary to the provisions or impair the basic rights and freedoms of the data subject that follow from the General Data Protection Regulation.

13. Entry into force and expiry

1. The provisions enter into force on the data of the parties' conclusion of an agreement on the supply of the services.

2. Both parties may require the provisions to be re-negotiated if law amendments or inadequacy of the provisions give rise to such amendments.

3. The provisions are in force as long as the service on processing of personal data lasts. For this period, the provisions cannot be terminated unless other provisions that regulate the supply of the service concerning processing of personal data, are agreed between the parties.

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller

The purpose of the data processor's processing of personal data on behalf of the data controller is the supply of a standard IT solution which, on the basis of the customer's reports to the data processor performs payroll processing for the customer, in accordance with the agreement.

A.2. The data processor's processing of personal data on behalf of the data controller primarily concerns (the nature of the processing)

The processing of personal data is primarily on the attention to IT systems to handle the payroll administration of the data controller.

The data processor's processing of personal data on behalf of the data controller concerns payroll processing, and includes:

- calculation of employee pay,
- make all calculations and reports, and execute money transfers to SKAT, ATP, holiday and maternity funds, pension funds etc. on the customer's behalf,
- report statistics to the employers' association and Statistics Denmark on behalf of customer,
- send payslips to employee digital mailboxes
- store the customer's payslips in an electronic archive for five years after the end of the year in which the payslip is produced
- provide assistance for the start-up and creation of the customer and the employees and
- provide support and consulting services via telephone and online from Visma DataLøn and ProLøn's payroll consultants whenever the customer needs help.

The data processor does not develop or adapt DataLøn in relation to the customer's specific needs or wishes.

In addition, the data processor facilitates operation, testing, maintenance, development and fault correction of systems and applications.

In addition, the data processor gets a non-exclusive, royalty-free, perpetual and irrevocable right in accordance with applicable law to anonymise and aggregate the data controller's data and use of Visma DataLøn og ProLøn A/S's products and subsequently use them to:

- Improve, optimise and develop the data processor's current or future modules, products and functions and
- Prepare statistics on:
    - wage formation and wage development,
    - company and employee circumstances,
    - demographics,

  including for the purpose of future functions and products.

When personal data is anonymised, the data processor must ensure that no natural persons can be identified based on the information or in combination with other information, and that the information cannot be traced back to an identifiable or identified natural person. The anonymisation must be irrevocable.

A.3. The processing includes the following types of personal data about the registered

Types of personal data subject to processing under the agreement:

General personal data	Special categories of personal data
• Contact information such as name, address, email, telephone • Civil registration number • Job category, information on salary, working hours, absence, pension, tax, bank account • holiday pay settlement • pension settlement • tax settlement • account information • employee number	• membership of a trade union, in the special situations where the employee's trade union fee is deducted from the salary

When using Legal Consulting the below mentioned Special categories of personal data can be included in the legal case work, but only if the Customer provides the information to the Legal Consulting.

	Yes	No
Racial or ethnic origin, political opinions, religious or philosophical beliefs		x
Data concerning health	x	
Trade union membership	x	
Data concerning sex life or sexual orientation		x
Genetic data or biometric data		x
Personal data relating to criminal convictions and offenses	x	

A.4. The processing includes the following categories of data subjects

Categories of data subjects that are included in the processing:

- The data controller's (the customer's) end users
- The data controller's (the customer's) employees
- The data controller's (the customer's) contact persons

A.5. The data processor's processing of personal data on behalf of the data controller may be commenced once these provisions have entered into force. The processing is of the following duration

This agreement applies as long as the data processor processes personal data on behalf of the data controller in accordance with the supply agreement (the agreement).

Appendix B Sub-processors

B.1. Approved sub-processors

On entry into force of the provisions, the data controller has approved the use of the following sub-processors:

Name and address	Hosting country	Legal transfer mechanism if the sub-processor has access to personal data from countries outside the EU/EEA	Assists the data processor with
Atea A/S Lautrupvang 6 2750 Ballerup CVR no. 25511484	Denmark	Not applicable	Data storage of customer cases Payroll runs
BtB Consult ApS Greve Bygade 22 2670 Greve CVR no. 29195951	Denmark	Not applicable	Case processing etc. in connection with the data processor's supply of payroll administration and customer support
Cim Mobilty ApS Fælledvej 17 7600 Struer CVR no. 27913334	Denmark	Not applicable	Sending of emails and SMS in connection with logon Option of sending SMS
Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Ireland	Not applicable	Case management internal, mails and sharing information
Confluent.io 899 West Evelyn, Mountain View, CA 94041, USA.	The Netherlands	Not applicable	Encrypted transport of data during calculations for the purpose of payroll runs
Microsoft Azure, Microsoft Ireland Operations Ltd. Atrium Building Block B, Carmanhall Road, Sandyford Industrial Estate, Dublin 18, Ireland	The Netherlands Germany	Not applicable	Data storage Payroll runs - calculations Master data - hosting
Netcompany A/S Grønningen 17, 1 1270 Copenhagen K CVR no. 14814833	Denmark	Not applicable	Sending of electronic mail (Mit.dk) Printing and sending of letters
ONLINECITY.IO ApS Buchwaldsgade 50 5000 Odense C CVR no. 27364276	Denmark	Not applicable	Sending of SMS in connection with logon

Orca Security Ltd. 3 Tushia St., Tel Aviv, Israel, 6721803	Frankfurt	Not applicable	Security scans of cloud infrastructure
PostNord Strålfors A/S Hedegaardsvej 88 DK-2300 Copenhagen S CVR no. 10068657	Denmark	Not applicable	Conversion and delivery to e-Boks
Visma IT & Communications AS Karenslyst Alle 56 0277 Oslo Org. no.: 979207379	Norway	Not applicable	Hosting of files for case processing of customer cases Print servers
Visma e-conomic A/S Gærtorvet 1 1799 Copenhagen V CVR no. 29403473	Denmark	Not applicable	Infrastructure and networks
Visma Raet B.V. Plotterweg 38, 3821 BB, Amersfoort, UTRECHT the Netherlands	The Netherlands	Not applicable	E-arkiv - software and hosting

On commencement of the provisions, the data controller has approved the use of the following sub-processors for the described processing activity. The data processor may not - without the data controller's written approval - use a sub-processor for processing activity other than the one described and agreed or use another sub-processor for this processing activity.

B.2. Notice for approval of sub-processors

The data processor must inform the data controller in writing of any planned changes regarding addition or replacement of sub-processors and thus give the data controller the possibility of objecting to such changes.
Such notification must be given at one month's notice to the first day of a month.

If the data controller has objections to the changes, the data controller must notify the data processor thereof. The data controller may object only if the data controller has reasonable and specific reasons for this.

Objections to addition or replacement of sub-processors will not be a stay for the performance thereof. If the data controller has objections, both the data controller and the data processor are entitled to terminate the agreement in writing with effect from the time of commissioning a new sub-processor so that the change will not come into effect to the data controller.

Appendix C Instructions concerning processing of personal data

C.1. The subject of the processing/instructions

The data processor's processing of personal data on behalf of the data controller takes place through the data processor's performance of the processing activities that are described in appendix A

C.2. Security of processing

Article 32 of the General Data Protection Regulation stipulates that, in consideration of the level, the implementation costs and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Accordingly, the data processor is entitled and obliged to make decisions on which technical and organisational security measures should be implemented to establish the necessary (and agreed) security level.

The information security of the data processor is based on the ISO 27001 framework.

The standard includes a Statement of Applicability (SOA), which is part of the data processor's Visma Dataløn Information Security Management System (ISMS).

Policies, procedures, processes, organisational decision-making processes and activities within the following information security control areas have been implemented:

- Information security policies
  - General guidelines and information security requirements
- Organisation of information security, including appointed
  - Information Security Manager and Data Protection Manager,
  - implemented Information Security Board.
- Employee security, including
  - background checks,
  - review of criminal record certificate,
  - declarations of confidentiality,
  - awareness training
- Management of assets, including
  - a register of assets and a classification thereof
- Access control, including
  - restriction of access to data based on a work-related need to the effect that obligations under the agreement can be met
- Cryptography, including
  - encryption or anonymisation of data
- Physical protection and protection of environment, including
  - protection of physical access routes to the data processor's premises
- Operational reliability, including
  - implemented processes for handling of development and change management,
  - backup,
  - logging,

    - monitoring of and protection against technical vulnerabilities.

- Communication security, including
    - protection and division of networks
    - established secure communication types.

- Acquisition, development and maintenance of systems, including
    - procedure for secure development

- Supplier conditions, including
    - procedure to secure that suppliers live up to the same obligations as set out in this data processing agreement,
    - procedure for ongoing follow-up.

- Management of information security breaches and personal data breaches, including
    - "Incident response" process,
    - procedure for informing the data controller.

- Information security aspects of emergency, preparedness and restoration management, including
    - implemented Business Continuity Management process

- Compliance, including
    - procedure for identification of legislation or contractual requirements.

If the data controller requests information on security measures, documentation or other forms of information on how the data controller processes personal data, and this information exceeds the standard information, described in C.7 of the provisions, made available by the data processor for the observance of applicable legislation on the processing of personal data as a data processor, and this results in additional work for the data processor, the data processor is entitled to request payment from the data controller for such additional work.

C.3. Assistance to the data controller

The data processor must, to the greatest extent possible, assist the data controller in accordance with provisions 9.1 and 9.2, including assisting the data controller with the following information in case of an information security breach.

- Description of the incident
- Identification of the data subjects affected by the incident
- Types of personal data included by the incident

The Data Processor does not respond directly to inquiries from Data Subjects, unless there is consent from the Data Controller. The Data Processor does not pass on personal data to public authorities, such as the police, unless there is a legal basis.

C.4. Storage period/erasure routines

Personal data is stored and erased as specified in Appendix D.

On expiry of the service concerning processing of personal data, the data processor must either erase or return the personal data in accordance with provision 11.1, unless after acceptance of these provisions, the data controller has changed its initial choice. Such changes must be documented and stored in writing, including electronically, in relation to the provisions.

C.5. Location of processing

Processing of the personal data covered by the provisions, may not without the data controller's prior written approval take place at other locations that the following:

Visma DataLøn og ProLøn A/S
Gærtorvet 1-5,
DK-1799 Copenhagen V

and with sub-processors as specified in appendix B.

In case of remote working, the processing of personal data can only take place by a connection via VPN (Virtual Private Network).

C.6. Instructions on transfer of personal data to third countries

The data controller provides instructions for personal data to be processed by the sub-processors mentioned in appendix B, and the said locations in the appendix.

If the data controller does not, in these provisions or subsequently, provide documented instructions concerning transfer of personal data to a third country, the data processor is not entitled to make such transfers within the framework of these provisions.

If the data controller does not, in these provisions or subsequently, provide documented instructions concerning transfer of personal data to a third country, the data processor is not entitled to make such transfers within the framework of these provisions.

C.7. Procedures for the data controller's audits, including inspections, in the processing of personal data assigned to the data processor

The data processor annually obtains an audit opinion from an independent third party regarding the data processor's compliance with the General Data Protection Regulation, data protection provisions in other EU law or the national laws of member states and these provisions.

The parties agree that the following types of audit opinions can be used in accordance with these provisions.

- ISAE 3000 GDPR audit report

According to agreed terms, the audit opinion can be sent to the data controller for information.

Based on the results of the declaration, the data controller is entitled to request the implementation of further measures for the purpose of ensuring compliance with the General Data Protection Regulation, data protection provisions of other EU law or the national laws of member states and these provisions. The parties must agree on any further measures. The data processor is entitled to terminate the agreement between the parties if an agreement cannot be reached. The data controller pays all costs in connection with further control, including payment for time spent by the data processor.

To make a request for the performance of an inspection, the data controller must submit a detailed inspection outline at least four weeks prior to the suggested inspection date to the data processor with a description of the suggested scope, duration and start date of the inspection.

The data controller or a representative of the data controller also has access to make inspections, including physical inspections, at the premises from which the data processor processes personal data, including physical premises and systems that are used for or in connection with the processing. Such inspections can only be made according to agreement between the parties.

If processing takes place in a multi-tenant environment or the like, the data controller authorises the data processor to decide, for security reasons, to have the inspections carried out by a neutral third-party inspector appointed by the data processor.

The data controller pays all costs related to such inspections.
In any case, inspections must be carried out within normal working hours at the site under the data processor's policies and may not unreasonably interfere with the data processor's business operations.

Any special remuneration for the data processor under the above is calculated based on the time spent by the data processor for obtaining information, and the data processors usual hourly rates in force, and in addition the data processor has the right that the data processor covers any external costs paid by the data processor for obtaining information, including costs paid for any required assistance from sub-processors.

C.8. Procedures for audits, including inspections, in the processing of personal data assigned to sub-processors

Based on risk assessments, the data processor annually obtains documentation for relevant sub-processors' compliance with the General Data Protection Regulation, data protection provisions of other EU law or the national laws of member states and these provisions. The parties agree that a procedure for the implementation and adequacy thereof is documented via the data controller's audit of the data processer, see C.7.

If further information about the sub-processors' compliance with the General Data Protection Regulation, data protection of other EU law or the national laws of member states and these provisions is to be provided to the data controller, the data processor will at the data controller's expense obtain the agreed required and accessible documentation from sub-processors.

Appendix D Deletion of data in Dataløn and E-arkiv

Data in DataLøn and E-arkiv is deleted according to the following rules:

DataLøn

D.1. Employee data in DataLøn

During employment: All data, including the event log and reports are stored for 6 years. Deletion takes place every day, when 6 years have passed.

After Resignation: All data of resigned employees is deleted after 1 year of inactivity. This means that the master data of the employees stays in DataLøn for 1 year + the current year after resignation.

The deletion takes place every year in January.

After termination of the Agreement: All data about the employees is deleted 9 months after termination of the agreement unless the company is enrolled for statistics. In that case, the information is deleted at the end of the first quarter of the year following the termination of the agreement.

The deletion takes place every month.

D.2. User access in DataLøn

The customer administers user access. If a right is taken away, the access is immediately closed.

However, the user access itself is not entirely deleted immediately.
This is due to the fact that a user's access may be related to other services of Visma's portfolio.

However, a user who has been inactive for 500 days will be deleted.

DataLøn login information is deleted 45 days after the termination of the agreement .

D.3. Company data i DataLøn

All data, including the event log and reports are stored for 6 years. Deletion takes place every day, when 6 years have passed.

After termination of the Agreement: All data about the Customers company is deleted 9 months after termination of the agreement unless the company is enrolled for statistics. In that case, the information is deleted at the end of the first quarter of the year following the termination of the agreement.

The deletion takes place every month.

D.4. Reported salary information in DataLøn

All data, including the event log and reports are stored for 6 years. Deletion takes place every day, when 6 years have passed.

After termination of the Agreement: All data about the Customers company is deleted 9 months after termination of the agreement unless the company is enrolled for statistics. In that case, the information is deleted at the end of the first quarter of the year following the termination of the agreement.

The deletion takes place every month.

E-arkiv

D.5. E-arkiv

Documents in E-arkiv are deleted after five years + current year, according the Danish Bookkeeping Act.

However, it should be noted that documents filed by the customer are not covered by the automatic erasure rules. These documents must be deleted by the Customer.

D.6. E-arkiv after termination of the agreement

All documents are deleted 9 months after the month in which the agreement is terminated.

If the Customer wants a copy of the documents in e-arkiv, the Customer can choose to download the documents or have them sent on a USB stick against invoicing.