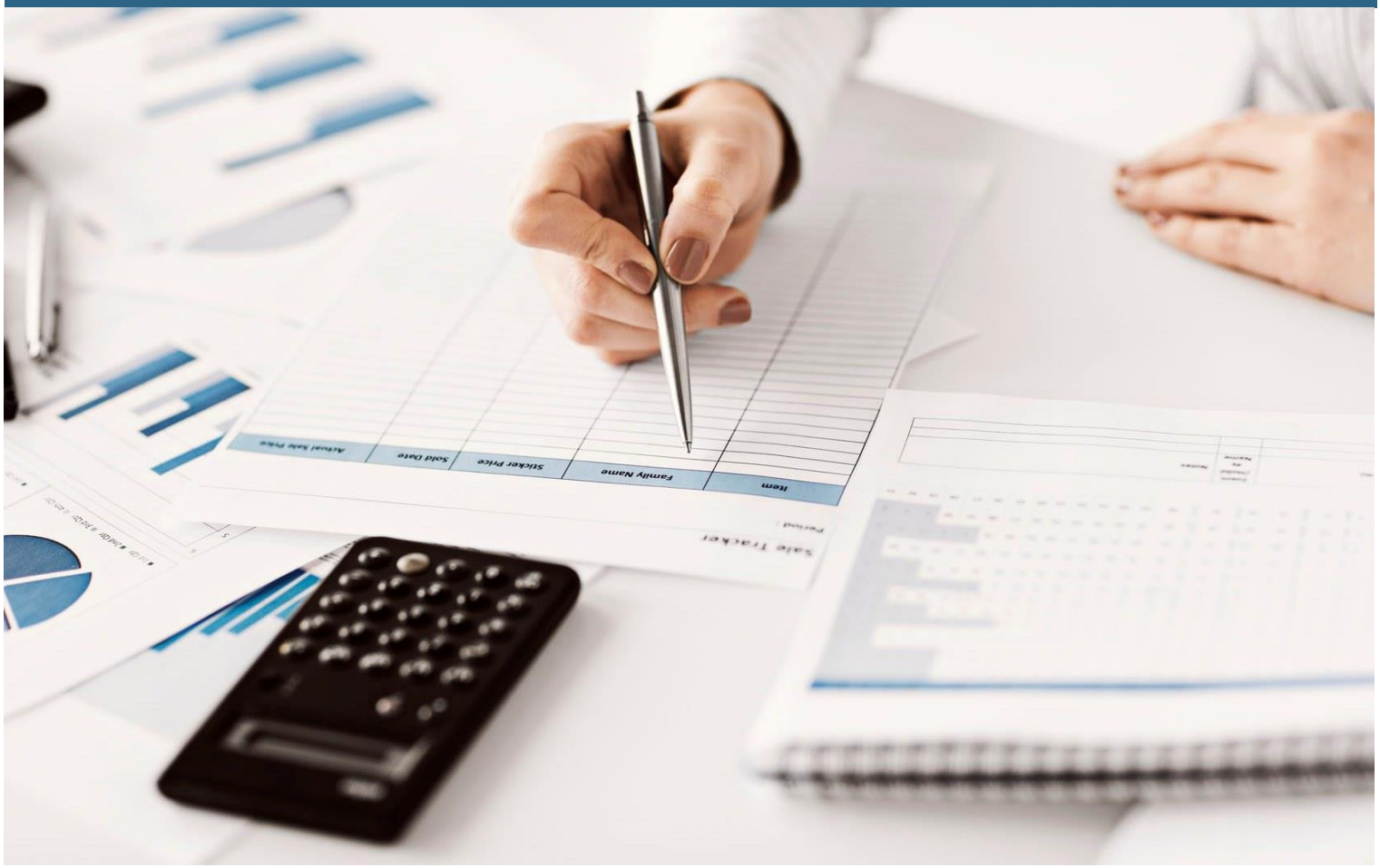
DATALØN



Terms and conditions for DataLøn

In force from 25 May 2018

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 and arrange for money transfers to SKAT, ATP (Labour market pension), holiday funds, maternity funds, pension funds, etc. on behalf of the Customer;
- reporting statistics to employers' associations and Statistics Denmark on behalf of the Customer;
- sending payslips to the Employees' e-Boks;
- 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.

Depending on the subscription type, DataLøn also contains a staff administrative manual, advice on employment law, and templates for staff 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. Agreement

These terms and conditions for DataLøn, including appendices and the Price List. The Agreement constitutes the overall contractual basis between Visma DataLøn and the Customer in relation to DataLøn.

2.2 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.

2.3 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.

2.4 DataLøn

Reference is made to condition 1.

2.5 dataløn.dk

The content available at www.dataløn.dk from time to time.

2.6. Primary 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.

2.7 The Customer

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

2.8. Employees

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

2.9 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.

2.10 Overførselsservice (Transfer Service)

Overførselsservice is a product provided by Nets Denmark A/S, whereby Nets Denmark A/S, on behalf of the Customer, processes and forwards the Payment Basis to the Customer's bank for the purpose of transferring money to the payee.

2.11 Price List

Visma DataLøn's price list for DataLøn in force from time to time which is available on dataløn.dk.

2.12 Samlet Betaling (Collective Payment)

ATP administers Samlet Betaling which, on signing the Agreement, covers calculation and collection of contribution for AUB, 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.

2.13 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, Sunday/public holiday allowance, and elective scheme.

2.14 Visma DataLøn

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

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 no concern of 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 authorises Visma DataLøn to make requests about the Customer's registrations in relation to eIndkomst and 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 Nets Denmark A/S for the use of Overførselsservice.

4.3 Employee Master Data

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

4.4 Primary Data

The Customer must provide the Primary Data to DataLøn as described at dataløn.dk under DataLøn via (i) the Customer entering it directly into DataLøn, or (ii) forwarding the Primary Data to Visma DataLøn in a format to be found at dataløn.dk, including in relation to format, set-up, contents, and deadlines.

4.5. Customer's IT equipment

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

4.6 Customer liability

The Customer is liable for all transactions, which the Customer, the Employees or others outside Visma DataLøn have made via DataLøn, to include in case of unauthorised use.

4.7 Customer storage

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

If the Customer wants to save templates for staff administrative work (depending on the subscription type), provided by Visma DataLøn and filled in by the Customer, the Customer must store such templates as Visma DataLøn does not store such material.

4.8 Customer information

The Customer is obliged to ongoing to 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. Price list

Visma Dataløn's services will be invoiced according to the Price List 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.
- 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 offence.

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. Storing Primary Data

Visma DataLøn shall store the Primary Data, pursuant to condition 4.3, for a minimum of 45 days and otherwise in accordance with the General Data Protection Regulation and the Danish Act on Processing of Personal Data. Visma DataLøn also stores a copy of the supporting documents created by Visma DataLøn as part of the salary processing (salary and bookkeeping data) for the remainder of the year plus five years, calculated from the time of production, after which the data is deleted.

Visma DataLøn records telephone conversations between the Customer and Visma DataLøn customer centres in order to be able to document the content of the conversations. The recordings are stored for 6 months, after which they are deleted.

10. Liability and disclaimer

10.1 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 suppliers, 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 Primary 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 e-Boks.

10.2 Properties of templates for staff 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.

10.3 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.

10.4 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 10 and 22 will apply in the widest possible sense permitted by Danish law.

Visma DataLøn's total liability for any single claim under this Agreement is limited to (i) 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 10.4 does not, however, apply to compensation paid by Visma DataLøn in accordance with condition 22 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.

11. Defects and delays

11.1 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.

11.2 Delays

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

11.3 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.

11.4 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.

11.5 Claims

Claims against Visma DataLøn as a result of defects or delays of which the Customer has given due notice, see condition 11.4, 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 11.4.

12. Licence

12.1 Customer's right of use

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.

13. 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 16.

14. Third-party rights

14.1 Infringement of third-party rights

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

14.2 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 10.

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 10.

The provisions in condition 14 do not apply to services from suppliers, see condition 16.

15. 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 fulfilment of the terms of the Agreement.

16. Use of other suppliers

16.1 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.

16.2 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.

17. Changes

17.1 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.

17.2 Changes to this Agreement

Visma DataLøn may change these terms and conditions for DataLøn, including the Price List, at one month's written notice to expire on 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 accounting voucher.

18. Termination and cancellation

18.1 Termination

The Customer may terminate the agreement at one month's written notice to expire on the first day of any month. Visma DataLøn may terminate the agreement at three months' written notice to expire on the first day of any month.

18.2 Cancellation

The Agreement may be cancelled 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 Nets Denmark A/S 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 11.1, or written demand to commence delivery, see clause 11.2, 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.

18.3 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.

19. 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 DataLøn group without the consent of the Customer.

20. 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 Price List.

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.

Additional terms and conditions for employment law advice

DataLøn customers have access to employment law advice, 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:

21. What is employment law advice?

General and specific telephone and/or written legal advice on employment law issues based on information from the Customer, see the current description of services for employment law advice.

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 counselling.

22. Disclaimer

In relation to liability arising from employment law advice, the third section of condition 10.4 above is replaced by the following.

If, as a result of the provision of employment law 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 Processor Agreement

1. Introduction

The following Data Processor Agreement between the Data Processor, Visma DataLøn A/S and the Data Controller, the Customer, shall form part of the Agreement between the Parties unless otherwise explicitly stated in other agreements between the parties.

The objective of the Data Processor Agreement is to regulate how and for what purposes the Data Processor shall process Personal Data on behalf of the Data Controller and to ensure that the Data Controller's Personal Data are processed in accordance with the Data Controller's guidelines and instructions as well as relevant data protection legislation.

Categories of Data Subjects and Personal Data being processed can be seen in Appendix A.

2. Definitions

Personal Data, Special Categories of Personal Data (Sensitive Personal Data), Processing of Personal Data, Data Subject, Data Controller, and Data Processor shall be defined as follows from relevant legislation regarding personal data processing, including the Data Protection Regulation (GDPR).

3. Data Controller's obligations

The Data Controller is responsible for the processing of Personal Data complying with the requirements of the Data Protection Regulation and the Data Protection Act.

The Data Controller, is obligated, when using the services made available by the Data Processor pursuant to the Agreement, to process Personal Data in accordance with relevant legislation regarding the processing of personal data.

The Data Controller is, i.a., responsible for ensuring that a statutory basis exists for the processing which the Data Processor is instructed to carry out.

4. Data processor's obligations

That Data Processor only processes Personal Data on behalf of and as instructed by the Data Controller.

Data processing must be performed as follows:

- Only in accordance with relevant legislation;
- For the purpose of fulfilling all obligations pursuant to the Agreement;
- As specified via the Data Controller's normal use of the Data Processor's services;
- As indicated in this Data Processor Agreement.

The Data Processor shall inform the Data Controller immediately if an instruction, in the opinion of the Data Processor, is in violation of the General Data Protection Regulation or data protection provisions of other Union law or Member State law.

The Data Processor must ensure that the Personal Data is subject to confidentiality, integrity, and accessibility in accordance with relevant legislation regarding the processing of personal data.

The Data Processor and their employees must maintain confidentiality regarding the Personal Data processed. This obligation also applies after the expiry of the Agreement.

The Data Processor shall ensure that the persons authorised to process personal data on behalf of the Data Controller have undertaken to observe confidentiality or are subject to an appropriate statutory duty of confidentiality.

The Data Processor shall assist the Data Controller with appropriate technical and organisational measures, where possible, for the fulfilment of the Data Controller's obligations regarding responding to requests from Data Subjects and regarding general execution of Data Subject rights pursuant to the Data Protection Regulation, Chapter 3 and Articles 32 to 36.

The Data Processor shall, without undue delay, notify the Data Controller of events about which the Data Controller is obligated to notify the Data Protection Agency or the Data Subject pursuant to legislation.

The Data Processor shall also, as far as this is appropriate and legal, notify the Data Controller of:

- Requests for the transfer of Personal Data from a Data Subject;
- Requests for the transfer of Personal Data from public authorities, e.g. the police.

The Data Processor shall not respond directly to enquiries from Data Subjects unless the Data Controller has provided their written consent. The Data Processor shall not transfer Personal Data to public authorities, e.g. the police, unless there is a legal basis for doing so.

The Data Processor shall not enjoy ownership of or control with whether or how the Data Controller elects

to use any third party's integrations with Data Processor API, via direct database link or similarly. The responsibility for such integrations with third parties rests with the Data Controller alone.

5. Security

The Data Processor must implement system, organisational, and technical measures to ensure a suitable security level with consideration to technology and implementation costs relative to the risks involved in the processing and the type of Personal Data to be protected.

The Data Processor is obligated to ensure a high level of security in their products and services. The Data Processors shall supply this level of security via organisational, technical, and physical measures in accordance with the information security measures requirements specified in the Data Protection Regulation, Article 32.

Additionally, the internal frameworks for the protection of personal data created by the Visma group are intended to ensure the confidentiality, integrity, security, and accessibility of personal data. The following measures are particularly important in this context:

- Classification of Personal Data with a view to implementing security measures commensurate with risk assessments.
- Assessment of the use of encryption and anonymising as risk-reducing measures.
- Limiting the access to Personal Data to those parties who need access to fulfil obligations pursuant to the Agreement.
- Control systems which register, recreate, prevent, and report breaches in connection with the processing of Personal Data.
- Security procedures as indicated in Appendix C.

If the Data Controller requests information regarding security measures, documentation, or other types of information regarding the handling of Personal Data by the Data Processor and this exceeds the standard information made available by the Data Processor in order to comply with relevant legislation regarding the processing of Personal Data as Data Processor, and this leads to additional work for the Data Processor, the Data Processor shall be entitled to require payment from the Data Controller for such additional work.

The Data Processor shall, without undue delay, notify to the Data Controller after becoming aware of a personal data security breach with the Data Processor or any Sub-Data Processor.

6. Control

The Data Controller may perform controls to ensure that the Data Processor complies with this Agreement up to 1 timer per year.

If it is mandatory requirement resting on the Data Controller, the Data Controller may request more frequent controls.

To request a control, the Data Controller must submit a detailed control list to the Data Processor at least four weeks prior to the proposed control date with a description of the proposed scope, duration, and start time for the control.

If third parties are to perform the control, this must as a general rule be agreed between the Parties. If processing is being performed in a "multitenant" environment or similar, the Data Controller shall permit the Data Processor to determine, for reasons of security, that the controls must be performed by a neutral third party controller selected by the Data Processor.

If the requested control scope is included in ISAE, ISO, or similar security report, performed by a qualified third party controller within the previous 12 months, and the Data Processor confirms that no significant changes have been performed to the controlled measures, the Data Controller shall confirm that such results are acceptable rather than request a new control of the measures covered by the report.

Controls must in any case be performed during regular working hours of the location in question pursuant to the Data Processor's policies and must not unreasonably affect the Data Processor's business operations.

The Data Controller shall cover all costs in connection with controls requested by the Data Controller.

Additionally, the Data Processor shall invoice the Data Controller for assistance in excess of the standard service which the Data Processor or the Visma group make available for the compliance with relevant personal data protection legislation.

7. Use of sub-data processors and transfer of data

As part of the delivery of services to the Data Controller, the Data Processor shall have the Data Controller's general permission to use sub-data processors. These sub-data processors may be other companies of the Visma group or external third party suppliers.

The Data Processor must ensure that sub-data processors are subject to the same obligations as are

detailed in this Data Processor Agreement. Any use of sub-data processors is subject to the Visma group Privacy Statement.

The Data Controller shall be entitled to request receiving an overview of sub-data processors currently used with access to Personal Data as indicated in Appendix B. The Data Controller shall also be entitled to request a full overview and more detailed information regarding such sub-data processors.

The Data Controller must be notified in advance of any changes of sub-data processors who process Personal Data. The Data Controller may only object if the Data Controller has reasonable, specific reasons for doing so.

The Data Processor must not allow the processing of Personal Data outside EU/EEA without the Data Controller's consent.

If the Data Controller gives consent for the Data Processor's processing of Personal Data outside EU/EEA, this will be indicated in Appendix B. The Data Processor must ensure the presence of a proper legal basis for the transfer of Personal Data outside of EU/EE on behalf of the Data Controller, to include concluding the EU Commission Standard Contract or transfer of Personal Data pursuant to Privacy Shield.

8. Term and termination

This Data Processor Agreement shall be in force for as long as the Data Processor processes Personal Data on behalf of the Data Controller in accordance with the Agreement. The Data Processor Agreement shall automatically terminate on notice of termination of the Agreement.

At the termination of this Agreement, the Data Processor shall delete, return, or store the Personal Data processed on behalf of the Data Controller as agreed with the Data Controller.

Unless otherwise agreed in writing, costs for such measures shall be based on:

- Hourly rate for the time spent by the Data Processor, and
- The degree of difficult of the requested processing.

The Data Processor may retain Personal Data subsequent to the termination of the Agreement in the extent this is a mandatory requirement, which shall be covered by the same technical and organisational security measures as described in this Data Processor Agreement.

9. Changes and additions

Changes to this appendix must be prepared in the form of a new appendix to the Agreement.

If any clause of this Data Processor Agreement should become invalid, this shall not affect the validity of the remaining clauses. The Parties shall replace the invalid clause with a valid clause reflecting the purpose of the invalid clause.

10. Liability

Liability for breaches to the clauses of this Data Processor Agreement shall be regulated by the liability clauses in Terms for DataLøn. This shall also be the case for breaches by the Data Processor's sub-data processors.

Sub-appendix A - Categories of Personal Data and Data Subjects

1. Categories of Data Subjects and Personal Data subject to processing pursuant to this Agreement

a. Categories of data subjects
   i. The Customer's end users
   ii. The Customer's employees
   iii. The Customer's contact persons

b. Categories of personal data
   i. Contact information such as name, address, mail, telephone
   ii. CPR No. (Civil reg. No.)
   iii. Job category, salary information, working hours, absence, pension, tax, bank account
   iv. Any other personal information required for the Data Controller to administrate the employment relationship.

c. Processing activities
   The Data Processor applies IT system to process the Data Controller's payroll administration, prepare salary slips, store and archive Personal Data regarding the Data Controller and the Data Controller's employees, reporting and transfer of data to the Data Controller, Nets Danmark A/S, banks, pension companies, any mandatory reports to employer's associations, public authorities (SKAT, statistics, etc.).

In addition, the Data Processor handles the operation, testing, maintenance, development, and error correction of systems and applications.

2. Types of sensitive personal data subject to processing pursuant to the Agreement

The Data Controller must notify the Data Processor about, and indicate below, any types of sensitive personal data in accordance with relevant legislation regarding the processing of personal data.

The Data Processor shall, on behalf of the Data Controller, process data about:	**Yes**	**No**
Race or ethnic, political, philosophical, or religious beliefs		X
That a person is the suspect in, charged with, or convicted of a crime.		X
Medical information		X
Sexual preferences		X
Union membership		X
Genetic or biometric data		X

Sub-appendix B - Overview of current sub-data processors

The Data Processor's current sub-data processors which may have access to the Data Processor's Personal Data at the conclusion of this Agreement comprise:

Name	Location/country	Legal transfer mechanism if the sub-data processor has access to personal data from countries outside of the EU	Assists the Data Processor with
Nets Denmark A/S Lautrupbjerg 10 2750 Ballerup CVR 20016175	Denmark	Not relevant	Data storage Payroll processing
Atea A/S Lautrupvang 6 2750 Ballerup CVR 25511484	Denmark	Not relevant	Data storage
Solipsis Marktplein 2 5306 BA Brakel	The Netherlands	Not relevant	Data storage, E-archive
NetNordic Enterprise Communications A/S Lyskær 1 2730 Herlev CVR 29797056	Denmark	Not relevant	Data storage, telephone conversations
Cohaesio A/S Per Henrik Lings Allé 4, 4. 2100 Copenhagen O CVR 26079209	Denmark	Not relevant	Infrastructure
Visma ITC AS Karenlyst alle 56 0277 Oslo	Norway	Not relevant	Infrastructure
OnlineCity ApS Buchwaldsgade 50 5000 Odense C CVR 27364276	Denmark	Not relevant	Sending SMS in connection with logging on
Cim Mobilty Fælledvej 17 7600 Struer CVR 27913334	Denmark	Not relevant	Sending SMS in connection with logging on
Visma Labs SIA Sporta Street 11 Riga LV 1013 Latvia	Latvia	Not relevant	Development and error correction

For Customers with subscription type "LønAdministration" (Payroll Administration), the following current sub-data processors may also have access to the Data Controller's Personal Data:

BtB Consult ApS Greve Bygade 22 2670 Greve CVR 29195951	Denmark	Not relevant	Case-handling etc. in connection with the Data Processor's delivery of payroll administration
Viborg Erhvervsservice ApS Gl. Skivevej 73 A 8800 Viborg CVR 21522783	Denmark	Not relevant	Case-handling etc. in connection with the Data Processor's delivery of payroll administration

Sub-appendix C - The Data Processor's security procedures

Security procedures

The information security of Visma DataLøn is based on the standard ISO / IEC 27001: 2013 Information Technology - Security techniques.

The standard includes Statement of Applicability (SOA) which forms part of Visma DataLøn Information Security Management System (ISMS). SOA comprises policies, procedures, processes, organisational decision-making processes, and activities of the following information security control areas of Visma DataLøn:

- Organisation of information security
- Employee security
- Asset management
- Access control
- Cryptographic controls
- Physical security and environmental security
- Operation security
- Communications security
- Acquisition, development, and maintenance of systems
- Supplier relationships
- Management of information security breaches
- Information security aspects of emergency preparedness and re-establishment management
- Compliance

Security of information

Visma DataLøn has implemented policies, controls, and processes to cover the information security areas described below:

- **Confidentiality**

To ensure that unauthorised persons cannot gain access to data which could be abused to the detriment of Visma DataLøn's customers, business relations, and employees.

- **Integrity**

To ensure that systems contain accurate and complete information.

- **Accessibility**

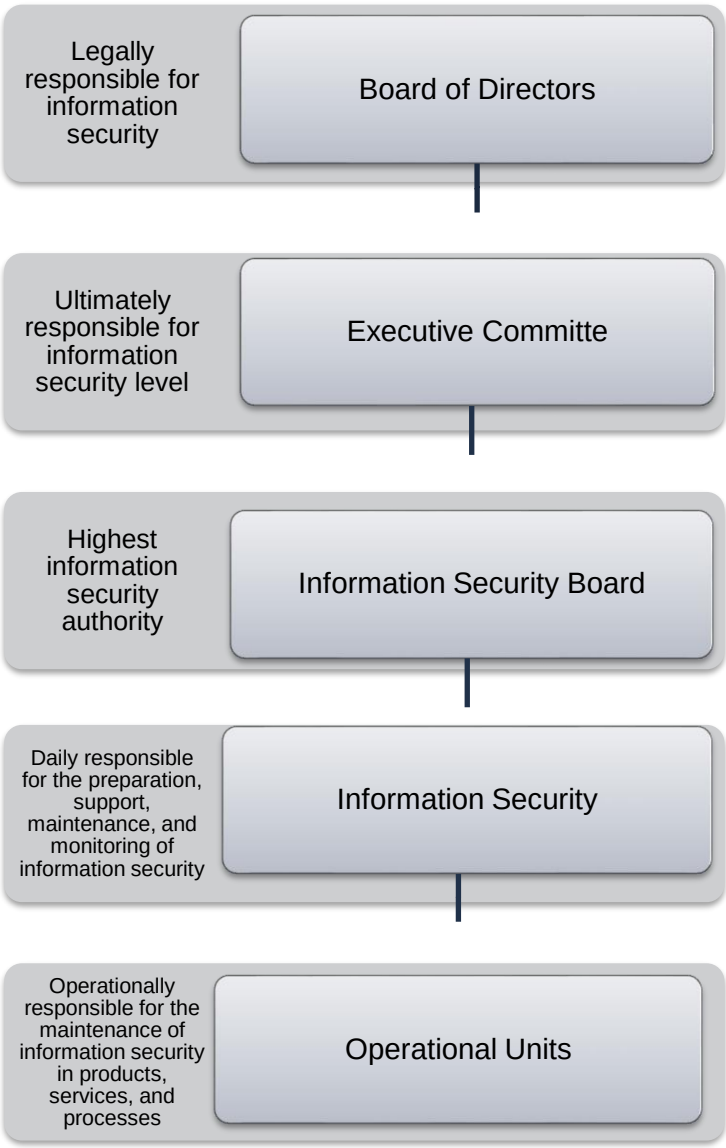
To ensure that relevant information and relevant systems are accessible and stable.

Information security management

Information security management at Visma DataLøn is based on ISO 27005 Information Technology - Security techniques - Information Security Risk Management.

Information Security - Organisation

Visma DataLøn has established a management framework for the initiation and management of information security implementation and operations.



Employee security

Visma DataLøn has ensured that employees and agreement partners understand their responsibilities and have the competencies required to fulfil their roles.

Asset management
Visma DataLøn has identified organisational assets and defined appropriate protection.

Access control
Visma DataLøn has, via approval and authorisation processes, ensure that it is only possible to gain work-related access to data and data processing facilities.

Cryptographic controls
Visma DataLøn has ensured correct and effective use of cryptography for the protection of the confidentiality, authenticity, and integrity of information.

Physical security and environmental security
Visma DataLøn prevents unauthorised physical access, damage, and disruption to the company's information and data processing locations.

Operational reliability
Visma DataLøn has ensured correct and secure operations via documented procedures and processes.

Communications security
Visma DataLøn has ensured the protection of information on networks and at data processing locations.

Acquisition, development, and maintenance of systems
All external acquisition or improvement/renewal of information systems, services, and components at Visma DataLøn is centrally assessed and approved for the purpose of ensuring compliance.

Policy for development and maintenance of services has been established and is used for the development in the organisation.

Supplier relationships
Visma DataLøn has ensured the protection of the company's assets accessible to suppliers, including regular monitoring and auditing of supplier deliveries.

Management of information security breaches
Visma DataLøn has a consistent and effectual approach to the management of information security incidents, including communications regarding security incidents and weaknesses.

Information security aspects of emergency preparedness and re-establishment management
Visma DataLøn ensures continuity and timely re-establishment of business-critical processes and systems in case of a critical situation and ensures that critical processes function at an appropriate level.

Compliance
Visma DataLøn has implemented procedures for the prevention of breaches to legal, legislative, or contractual obligations in connection with information security and any security requirements.