The Ministry of Social Affairs and the Interior

Date: 11 May 2020
Section: CPR Administration
Ref.no.: 2018-321

Standard terms and conditions for CPR data deliveries from the Data Distributor to private enterprises and individuals

The Data Distributor is the controller of the Ministry of Social Affairs and the Interior for purposes of the Ministry's disclosure of CPR data via the Data Distributor.

Introduction

Under section 38(1) of the Danish Civil Registration System (CPR) Act, limited liability companies, foundations, enterprises and other legal persons as well as natural persons engaged in business activities are entitled to be provided by the Ministry with data from the civil registration system (the "CPR") concerning a large specified group of persons each of whom has been identified individually in advance by the relevant client. If the legal person is an association, its objects must be creditable.

Section 38(2)-(4) of the Act specify the data which are available under subsection (1).

Under section 40(1) of the Act, the Ministry lays down the terms and conditions, including on security measures and payment, governing disclosure of CPR data to private enterprises and individuals.

The provision by the Data Distributor of CPR data to private enterprises and individuals is subject to the recipient being entitled to process such data under the EU General Data Protection Regulation (the "GDPR") and the Danish Data Protection Act, see section 38(6) of the Danish Civil Registration System Act.

Accordingly, the processing of CPR data is only permitted if legal under Chapter II of the GDPR and under the Danish Data Protection Act, which means, among other things, that it must fulfil the data processing principles in article 5 concerning legitimacy (necessity), proportionality and updating.

By way of example, the requirements for legitimacy and proportionality mean that the fact that an enterprise is entitled/required under, for example, the Danish Bookkeeping Act to retain information about an individual does not in itself entitle the enterprise to continue to update the data subject's name and address data based on the CPR.

Any person who intentionally or with gross negligence violates these terms and conditions will be fined, unless a more severe penalty is due under other legislation, see section 57(1)(iv) of the Danish Civil Registration System Act.

Any matters relating to the processing of CPR data from the Data Distributor which are not governed

by these terms and conditions are governed by the GDPR and the Danish Data Protection Act and provisions laid down thereunder.

Notice of any amendments to these terms and conditions and current service updates will be given only through the news subscription service at www.datafordeler.dk.

1 Establishment and change of client relationship

Requests for access to CPR data on the Data Distributor within the scope of these terms and conditions must be submitted by the client to the Data Distributor via Datafordeler.dk. The intended purpose must be specified in the request.

When processing access requests, the CPR Administration will consider which CPR data on the Data Distributor may be accessed in order to ensure that the delivery from the Data Distributor does not include data on any more persons or any more data on such persons than necessary for the specified purpose and that the delivery is in compliance with the Danish Civil Registration System Act and the GDPR and the Danish Data Protection Act. The delivery time will depend on the product requested and the scope of the purpose.

2 Authorisation and access control

For access to CPR data from the Data Distributor via system-to-system solutions, the client must designate a security officer to be responsible for compliance with these terms and conditions and for ensuring that only employees with a work-related need to use the system-to-system solution are authorised to perform queries to the Data Distributor for CPR data via the solution.

For access to CPR data from the Data Distributor via system-to-system solutions, one user profile will usually be created (using the following designations on the data distributor: web user, service user and system user) at datafordeler.dk, from which a client designated certificate will be authorised to access CPR data. The client's security officer must ensure that the user profile as well as the certificate are in the enterprise's possession at all times.

The client must ensure that its employees use personal authorisation IDs in its own systems in connection with access to CPR data from the Data Distributor via system-to-system solutions.

The security officer must keep a list of the employees and the system-to-system solutions to whom or which authorisation has been granted, stating the date of authorisation and the date of expiry of the authorisation.

The client must ensure that all searches in CPR data from the Data Distributor via system-to-system solutions are registered to the individual employee's user ID in the client's system. It should be noted that the Data Distributor usually only registers the user ID and certificate of the client program that communicated with the Data Distributor.

The client must provide the security officer with a monthly statistical report of the use of CPR data from the Data Distributor via system-to-system solutions (transaction statistics) showing which

transaction types were used and how many times each individual transaction type was used. The statistical data, which will be used in cases of suspected abuse of access to CPR data from the Data Distributor, must be checked by the security officer.

If the CPR data from the Data Distribtor are accessed in connection with a self-service function at a website available to the public, the client must ensure that users of such service may perform queries in CPR data from the Data Distributor only after authentication using NemID, and that their civil registration numbers are verified through the PID-CPR Match of the Danish Agency for Digitisation.

3 Rules governing processing and disclosure by private enterprises and individuals of CPR data received from the Data Distributor

The client is the controller for the CPR data received by the client from the Data Distributor.

CPR data received by the client from the Data Distributor may be used only for the intended purpose.

Individuals may request protection of their names and addresses in the CPR, and those protected data are not available to private enterprises and individuals. However, credit rating agencies are entitled to receive data about names and addresses, regardless of whether they are protected.

CPR data obtained from the Data Distributor by private enterprises or individuals may not be disclosed to other private enterprises and individuals, unless provided by statute law or provisions laid down in pursuance of statute law. Protected names and addresses obtained by credit rating agencies from the Data Distributor may not be disclosed by such agencies.

If CPR data received from the Data Distributor are entrusted to a service agency or the like for processing purposes, it will not be deemed to be a disclosure to private enterprises or individuals, provided the data processor processes the data in compliance with the GDPR and the Danish Data Protection Act.

If the data processor is registered in this connection by the Data Distributor and approved by the CPR Administration as a recipient of the CPR data, the data processor must guarantee that agreements/measures are in place between the data controllers (enterprises etc., see section 38(1) of the Danish Civil Registration System Act) and the data processor to ensure that the data subjects are able to exercise their rights under the GDPR and the Danish Data Protection Act, including the rights which require knowledge of the data controller's identity. This means that, if so requested, information must be readily provided by the data processor to the data subjects as to which enterprises etc. receive CPR data on them from the Data Distributor via the data processor.

The data processor's processing of data must always be in compliance with these terms and conditions.

All CPR material, which must be kept in a locked cabinet or room or the like when not used, must be treated as confidential and any unauthorised access is therefore prohibited.

4 Client control of authorisations to the Data Distributor and queries in CPR data

The client must have internal regulations in place for ongoing and appropriate control of its authorisations to receive CPR data from the Data Distributor and its searches and queries via the CPR products on the Data Distributor. The regulations laid down by the client must reflect the actual facts and must be updated on a regular basis, but at least once a year.

If so requested by the CPR Administration, the client must be able to provide a copy of its internal regulations as well as documentation of the controls carried out.

The client's internal regulations on ongoing control must take into account that the client is required to carry out a control of its authorisations for CPR data from the Data Distributor at least every third month.

All searches and queries will be recorded by the Data Distributor. The details are recorded in the Data Distributor's logpoint solution and include details about the user (VID, MID, VOCES and MOCES), transaction type (service, file downloads, etc.), date and time as well as the data which the CPR query or search on the Data Distributor concerns. For system-to-system access, the client must record the transactions of each individual user in its own system.

Via the Data Distributor, the client's designated security officer users will have access to (i) a log search which enables the generation of a report showing selected or all searches and queries made by the client's own users (log search) and (ii) a usage statistics (transaction statistics) report. The statistical data show the types of transaction used by each individual user profile/certificate and how many times each individual type of transaction has been used.

The client's internal regulations on ongoing control must include a control based on the log search and the transaction statistics, respectively. The control performed must be able to show if the client's employees use authorisations on the Data Distributor in compliance with these terms and conditions as well as the GDPR and the Danish Data Protection Act. The control procedure must be performed at least every third month.

When using system-to-system access, the client itself is responsible for generating similar monthly statistics and performing similar ongoing controls.

If the client suspects any abuse of CPR access, the client must perform a control. Such control cannot replace the ongoing controls.

5 Requirements for data communication access

Reference is made to the terms and conditions of the Data Distributor, which include requirements for data accesses, requirements for encryption technologies, secure file transfers, connection technologies, etc.

In connection with establishment of access, time must be allowed for the client's IP addresses to be whitelisted by the Data Distributor operator.

6 Use of CPR data by private enterprises and individuals for statistical or research purposes

Reference is made to the Danish Health Data Authority, which is responsible for disclosure of CPR data for statistical or research purposes.

7 Payment

The costs in connection with CPR data deliveries from the Data Distributor are payable by the recipient private enterprise or individual. Payment must be made directly to the Agency for Governmental Administration, which handles invoicing on behalf of the CPR Administration.

Any questions and correspondence relating to invoicing should be submitted to the CPR Administration's customer service thru the CPR Servicedesk.

The fee for CPR data deliveries from the Data Distributor will be invoiced at the unit prices applicable from time to time. The fee is payable from the time when the Data Distributor has set up the necessary software/access to CPR data from the Data Distributor.

Unit prices are available on request from the CPR Administration.

The CPR Administration may request payment in advance, for example as an on-account payment.

If the client discloses CPR data received from the Data Distributor for commercial purposes, the CPR Administration reserves the right to charge a discretionary payment (royalty).

8 Maintenance and downtime

The CPR products from the Data Distributor are available 24 hours a day, seven days a week. For purposes of service and maintenance etc., the system may be shut down and downtime may thus occur for a few hours, usually during weekends. Notice of downtime will be posted at www.datafordeler.dk - reference is made to the Data Distributor operator for all enquiries concerning maintenance and downtime.

CPR products used for system-to-system solutions in particular are continuously adapted to meet the requirements of the surrounding world. Any changes in individual products will be subject to at least three months' notice. Any costs incurred by the client for any changes necessary in that connection are payable by the client.

9 Errors and defects

In the event of errors or defects in a data delivery from the Data Distributor, where such errors or defects are exclusively due to matters attributable to the Data Distributor, the Data Distributor will remedy such errors or defects without any undue delay.

If the Data Distributor duly remedies the errors or defects, the client will have no further claims relating to errors or defects.

10 Liability

The CPR Administration will have no liability for business interruption, loss of profit or any other indirect loss. The liability of the CPR Administration cannot exceed the amount paid in connection with access to CPR data from the Data Distributor.

11 Force majeure

If the CPR Administration or the client of the CPR is prevented from performing its obligations due to circumstances arising after the signing of the agreement, the CPR Administration or the client, as the case may be, will be entitled to cancel the agreement, unless the relevant party ought to have taken into account the circumstances preventing the performance of the agreement at the time when the agreement was made.

The CPR Administration acknowledges that the CPR service on the Data Distributor is essential, and the Data Distributor operator will therefore take all appropriate measures in order to ensure continuous service in the event of force majeure, including strikes and lockouts.

12 Disputes

Any dispute arising out of data deliveries from the Data Distributor to clients of the CPR will be resolved by arbitration according to the Rules of Arbitration Procedure of the Danish Institute of Arbitration.

Danish law will apply.

13 Termination

The client may terminate the agreement with the CPR Administration concerning access to CPR products on the Data Distributor by giving one month’s notice in writing to expire at the end of a month – but no earlier than three months after access has been established.

The CPR Administration may terminate the agreement concerning access to CPR services on the Data Distributor with immediate effect for breach of the agreed terms and conditions, including for default.

In connection with legislative changes, technological advances, efficiency improvement measures, etc., the CPR Administration may decide to implement changes concerning CPR data deliveries from the Data Distributor or phase out service products, output data, file deliveries, etc. subject to reasonable notice.