Date: 25 May 2018
Section: CPR Administration
Ref.no.: 2018-321

THE MINISTRY FOR ECONOMIC AFFAIRS AND THE INTERIOR

Standard terms and conditions for data deliveries from CPR to private enterprises and individuals (including private enterprises and individuals in Greenland)

(Applicable to all data deliveries, except for CPRWeb access)

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 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.

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 updating the data subject's name and address data based on the CPR.

The provision to private enterprises and individuals in Greenland of CPR data falling within the scope of Part 1 of the Danish Private Registers etc. Act is subject to the recipient being entitled to record such information under Parts 2-6 of the same Act, see section 38(6) of the Danish Civil Registration System Act.

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 personal data from the CPR 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.cpr.dk and news tickers in the CPR.

Establishment and change of client relationship

Requests for data deliveries from CPR and for any subsequent changes must be submitted by email to the CPR Administration at kc@cpr.dk. The intended purpose must be specified in the request.

When processing access requests, the CPR Administration will consider which CPR data may be accessed in order to ensure that the delivery from the CPR 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.

Requirements for data communication

Batch deliveries take place by file transfer only.

Data transfers must be effected in a manner which does not compromise data. The CPR Administration lays down the rules in this regard, which must include use of encryption and IP address verification, among other things.

Requests for new IP addresses are usually processed within 24 hours on weekdays, provided that the request is received before 12 noon on a weekday.

CPR access via system-to-system solutions must not be used for online batches without prior approval from the CPR Administration.

Authorisation and access control (applicable to system-to-system solutions)

For CPR access 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 CPR queries via the solution.

For CPR access via system-to-system solutions, one "system user ID" and one password will usually be issued for the client's program. The security officer must ensure that the password is changed to a confidential password when the program is used to access the CPR for the first time. The password must comply with the CPR Administration's password construction guidelines as stated in the standard terms and conditions for access by private enterprises and individuals to the CPR query/search system, CPRWeb.

The client must ensure that its employees use personal authorisation IDs in its own systems in connection with CPR access 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 CPR searches 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 CPR usually only registers the "system user ID" of the client program that communicated with the CPR.

The client must provide the security officer with a monthly statistical report of the use of CPR 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 CPR access, must be checked by the security officer.

If the CPR is 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 the CPR only after authentication using NemID, and that their civil registration numbers are verified through the PID-CPR Match of the Danish Agency for Digitisation.

Rules governing processing and disclosure of CPR data by private enterprises and individuals

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

CPR data received by the client from the CPR 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.

Data obtained from the CPR by private enterprises or individuals may not be disclosed to other private enterprises or 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 CPR may not be disclosed by such agencies.

If data received from the CPR 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 in the CPR 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. subscribe via the data processor for CPR data on them.

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.

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.

Marketing communications

The CPR data delivery may contain an indication to the effect that an individual has opted out of marketing communications.

Such an indication in the CPR provides protection against marketing communications under section 10 of the Danish Marketing Practices Act and protection against disclosure etc. by another enterprise for marketing purposes under article 21 of the GDPR and section 13(4) of the Danish Data Protection Act.

Payment

The costs in connection with CPR data deliveries are payable by the recipient 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 at kc@cpr.dk.

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

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 information received from the CPR for commercial purposes, the CPR Administration reserves the right to charge a discretionary payment (royalty).

Maintenance and downtime

The CPR is available 24 hours a day, seven days a week.

Batch deliveries will be made Mondays to Fridays after 6:00 pm, except on 5 June, 24 December and 31 December. In addition, special batch deliveries are available by separate agreement.

For purposes of service and maintenance etc., the system may be shut down for a short space of time, usually during weekends. Notice of downtime will be posted at www.cpr.dk and in news tickers in the CPR.

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.

Any transfer of the CPR service to another IT service provider 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.

Errors and defects

In the event of errors or defects in a data delivery, where such errors or defects are exclusively due to matters attributable to the CPR Administration, the CPR Administration will remedy such errors or defects and/or make a replacement delivery without any undue delay.

If the CPR Administration duly remedies the errors or defects and/or makes a replacement delivery, the client of the CPR will have no further claims relating to errors or defects.

Support is available from the CPR Administration and DXC Technology during business hours. The DXC Helpdesk may be contacted 24/7 at +45 36 14 61 92, but only for defects in the CPR system.

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 the CPR data delivery.

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 is essential, and the CPR Administration will therefore take all appropriate measures in order to ensure continuous service in the event of force majeure, including strikes and lockouts.

Disputes

Any dispute arising out of data deliveries from the CPR Administration 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.

Termination

The client may terminate the CPR data delivery agreement with the CPR Administration by giving one month's notice in writing to expire at the end of a month.

The CPR Administration may terminate the CPR data delivery agreement 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 and forms or phase out service products, output media, etc. subject to reasonable notice.