**THE MINISTRY FOR ECONOMIC AFFAIRS AND THE INTERIOR**

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

**Standard terms and conditions for access by private enterprises and individuals to the CPR query/search system, CPRWeb (including private enterprises and individuals in Greenland)**

Introduction

Under section 39 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 granted access by the Ministry to perform single queries (address queries) in the civil registration system (the "CPR"). If the legal person is an association, its objects must be creditable.

Section 42(1) and (2) of the Act specify the data which are available under section 39.

Under section 40(1) of the Act, the Ministry lays down the terms and conditions, including on security measures and payment, governing disclosure of data pursuant to section 39.

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 EU General Data Protection Regulation (the "GDPR") and the Danish Data Protection Act and provisions laid down thereunder.

It should be noted that in connection with the use of the CPR, users may be subject to a duty to provide certain information to the data subjects under the provisions of the GDPR.

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 CPRWeb access must be submitted by email to the CPR Administration's customer service at kc@cpr.dk.

When processing such requests, the CPR Administration will consider whether the conditions of the Danish Civil Registration System Act for access to electronic single queries as well as the rules on security measures have been satisfied, before the client is granted CPR access.

On establishment of access, the necessary access related information must be exchanged.

Authorisation and access control

The client must designate a security officer to be responsible for compliance with these terms and conditions and for ensuring that authorisation to perform CPR queries is granted to employees strictly on a need-to-know basis.

The CPR Administration will issue one or more administrator IDs (user ID and password) to the security officer, who will then order the required user IDs for relevant employees in the CPR. Each employee must be provided with a user ID with a secret password. When the individual employee logs on to the CPR for the first time, the password must be changed to a personal and confidential password which is only known to the relevant employee. When the employee surrenders the authorisation, the security officer must ensure that the password is changed to a confidential password known only to the security officer.

The security officer must keep a list of the employees to whom authorisation has been granted, stating the date of authorisation and the date of expiry of the authorisation. The list may be kept in the CPR using the features designed for this purpose.

The individual employees must observe the following password rules:

- The password must be personal
- The password must not be shared with or lent or disclosed to any other person
- The password must be changed after a maximum period of use of 90 days
- The password must be a minimum of eight characters long, consisting of:
- At least one lower-case letter (a-z)
  At least one upper-case letter (A-Z)
  At least one digit (0-9)
  At least one special symbol ~ ! @ # $ % ^ * ( ) _ - + = , . / \ { } [ ] ; :
- The password must not be reused
- The password must not contain any consecutive numbers (eg. peter001, peter002, etc.)
- The password must not consist of the employee's own or any family member's name or initials, birth date, personal registration number, licence plate number, car make or any other names or designations which are easy to guess
- The password must be changed if it has been or may have been disclosed to others
- Employees are not allowed to leave their terminal or the room without logging out of the CPR system.

The user will be disabled after five unsuccessful attempts at entering the correct password. If the user ID has been disabled or forgotten, it must be unlocked by the security officer or the person(s) authorised by the security officer for that purpose. The CPR Administration will assist in unlocking IDs only in special circumstances.

All queries will be logged in the CPR. The details will show user ID, date and time as well as the data which the CPR query concerns. These details will form the basis of a printed report in cases of suspected abuse of CPR access.

Via the CPRWeb, the users have access to terminal usage statistics (transaction statistics). The statistical data show the types of transaction used by each individual user and how many times each individual type of transaction has been used. Each month, the client's security officer must check the transaction statistics for the users to whom the security officer has granted authorisation.

When checking the employees' terminal system usage, the security officer is entitled, against payment of a fee, to request a list from CPR showing the terminal traffic for one or more user IDs for a specified limited period.

Requirements for data communication

There are no special data communication requirements. However, the network provider must be reputable. Data communications must be encrypted.

Rules governing client disclosure of CPR data

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

The client may not disclose data received from the CPR in connection with CPR access to other private enterprises or individuals, unless provided by statute law or provisions laid down in pursuance of statute law.

If a client entrusts data received from the CPR 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.

Individuals may request protection of their names and addresses in the CPR. The client's access to CPR data does not include protected names and addresses.

Marketing communications

The CPR response screen 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 the use of the CPR terminal systems are payable by the client. 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 use of the CPRWeb will be invoiced at the unit prices applicable from time to time. The fee is payable from the time when the CPR Administration has established 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 CPRWeb is available 24 hours a day, seven days a week.

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

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 CPR access, where such errors or defects are exclusively due to matters attributable to the CPR Administration, the CPR Administration will remedy such errors or defects without any undue delay.

If the CPR Administration duly remedies the errors or defects, 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 CPR access.

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, including the provisions of the GDPR and the Danish Data Protection Act.

Termination

The client may terminate the CPR access agreement with the CPR Administration 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 CPR access 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 the CPRWeb subject to reasonable notice.