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 access by public authorities

(including Greenlandic authorities)

1 Introduction

Pursuant to section 32(1) of the Danish Civil Registration System Act, a public authority which requires information recorded in the civil registration system (the "CPR") may retrieve such information from the CPR.

Pursuant to section 32(2) of the Act, the Ministry lays down the terms and conditions, including on security measures and payment, governing disclosure of information pursuant to subsection (1).

The provision of personal data from the CPR is subject to the public authority being entitled to process such information under the EU General Data Protection Regulation (the "GDPR") and the Danish Data Protection 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.

2 Establishment and change of client relationship

Requests for CPR access within the scope of these terms and conditions must be submitted by the public authority (the client) to the CPR Administration thru the CPR Servicedesk.

When processing access requests, the CPR Administration will consider which CPR data may be accessed by the client 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.

3 Authorisation and access control

The public authority must designate a security officer to be responsible for compliance with these terms and conditions and for ensuring:

- that internal regulations on security measures are established locally;
- that such security measures are observed;
- that CPR access is granted strictly on a need-to-know basis and that no employees are granted access for purposes for which they have no need;
- that access is granted only to employees who report data to the CPR (applicable to municipalities, registrars of church records of the Danish National Church, registrars of the civil registration system i Southern Jutland, the state administrations, the courts of law, the Nationality Division (*Indfødsretskontoret*) of the Danish Ministry of Integration, hospitals and the Danish tax authorities);
- that the data reported, for example a change of address, are reported by the proper person with a view to updating the CPR through a self-service server;
- that the employees are trained in the use of CPR access; and
- that the employees are familiar with the internal regulations on security measures and these terms and conditions.

When granting online CPR access, the CPR Administration will issue one or more user IDs with administration rights (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.

For system-to-system CPR access, however, only a single system user ID will be issued for use in 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 individual employee must use the authorisation ID issued by the client for his or her use in the client's system used for system-to-system CPR access.

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

In connection with CPR online access, 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 not be reused
- The password must comply with the applicable rules concerning valid characters
- 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

The user ID will be disabled after five unsuccessful attempts at entering the correct password. If the user ID has been disabled, 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 user IDs only in special circumstances.

The employees are only authorised to access data in the CPR which are necessary for performing their required functions and tasks, ie. data which form an inherent part of case processing.

Any use of the CPR for private purposes is strictly prohibited.

Employees are not allowed to leave their workstation or the room without logging out of the CPR or the CPR access system. Alternatively, they may lock their workstation so that it can only be unlocked by entering a personal password.

4 Client control of CPR authorisations and queries

The client must have internal regulations in place for ongoing and appropriate control of its CPR authorisations and its CPR searches, queries and updates. 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 CPR authorisation controls at least every third month.

All searches, queries and updates are recorded in the CPR. The details are recorded in the CPR system and show user ID, transaction type, date and time as well as the data which the CPR query, search or update concerns. For system-to-system access, the client must record the transactions of each individual user in its own system.

Via the CPR system (CPRWeb), the client's designated users will have access to (i) a log search which enables the generation of a report showing selected or all searches, queries and updates made by the client's own users (log search) and (ii) a usage statistics (transaction statistics) report.

The statistics show the types of transaction used by each individual user 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 CPR authorisations in compliance with these terms and conditions and the Danish Data Protection Act. The control procedure must be performed at intervals of no more than three months.

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

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

6 Requirements for client installations

In connection with TCP/IP connections, the client must ensure that the pools of IP addresses assigned to the client for traffic to and from the CPR are only used by the client or by other public sector clients with similar CPR access.

The client is responsible for complying with the following requirements:

- The administrative local area network must be safeguarded against any unauthorised third party access.
- Data sniffing on the administrative local area network must not be possible from PCs which are not part of the administration.
- For network purposes, the administrative local area network must be limited to other local area networks, including, for example, local area networks for visitor or student terminals.
- Administrative terminals and servers with TCP/IP connection to the CPR may not use the same IP address for outgoing TCP/IP traffic as non-administrative terminals, such as, for example, visitor or student terminals.

7 Requirements for home workstations (access from a home PC or the like to the client's local area network)

The security officer is responsible for ensuring compliance with the following guidelines:

- Special guidelines must be in place with respect to setting up home workstations in order to ensure compliance with the regulations on security measures.
- Rooms used in connection with home workstations must be fitted out in a way preventing unauthorised access to the data.
- Access from the home workstation to the client's local area network must comply with the provisions set out in the above section on data communication access.
- Unless encrypted, CPR data must not be stored on the home workstation.
- Where other use of the home workstation is authorised, for example private use, guidelines for such use and any necessary related security measures must be established.
- If data are printed from the home workstation, rules must be in place to ensure the safekeeping of the data to prevent unauthorised access, including rules on safe destruction.
- Guidelines for protecting the home workstation against virus attacks or other misuse must also be in place.
- A timeout feature must be activated if the home workstation is idle for ten minutes so that it is either locked and can only be unlocked with a password, or the connection to the CPR is terminated.
- The security officer oversees compliance with the special guidelines to ensure compliance with the regulations on security measures.

8 Client processing of civil registration numbers

Part 13 of the Danish Civil Registration System Act contains the following provisions on the processing of civil registration numbers by public authorities:

"52.- *(1)* If, in accordance with 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 the Danish Data Protection Act, a public authority uses a civil registration number as identification or case number, the civil registration number used shall be for the person whom the case concerns.

(2) The provision in subsection (1) shall not apply, however, if, according to statute law or provisions laid down in pursuance of statute law, it is necessary in a specific area of administration to record several persons under the same case. In such cases, the administration shall decide for itself the most appropriate organisation of internal case registration. In connection with this organisation, equal opportunities shall be taken into account.

53.- *(1)* A public authority using a civil registration number when contacting a person about his or her affairs shall use the civil registration number of the person concerned. Similarly, a person may only be asked to provide his or her own civil registration number when contacting public authorities in situations covered by section 52.

54.- *(1)* Public authorities shall ensure that there is no unauthorised access to civil registration numbers. Civil registration numbers may not be shown fully legibly on the outside of letters, in window envelopes or in other mail sent to the person concerned. If identification is required in such cases, the civil registration number shall be blurred such that it is not immediately recognisable.

(2) Civil registration numbers may be shown fully legibly on giro-payment slips provided these are sent to the person concerned in a sealed envelope.

(3) Civil registration numbers may not be made public, including in the Danish Official Gazette, except in notices to creditors in estates of a deceased person, unless provided by statute law or provisions laid down in pursuance of statute law."

9 Rules governing client processing and disclosure of data received from the CPR

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

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

The client may disclose data, including protected names and addresses, to other public authorities or private enterprises and individuals only if such disclosure is provided for 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 to the effect that their names and addresses may not be disclosed to private enterprises or individuals.

The client must ensure that protected names and addresses are not available to private enterprises or individuals. The client is required to register the information about the protection in all instances in connection with names and addresses. Furthermore, such information must always be provided in connection with any disclosure of names and addresses to other parties. This provision applies, unless otherwise provided by statute law or provisions laid down in pursuance of statute law.

The client is responsible for ensuring that there is no unauthorised access to CPR data. 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 Nets.

10 Client use of CPR data 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.

11 Payment

The costs in connection with CPR access are payable by the recipient authority. 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 use of the CPR 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 access to the CPR.

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).

12 Maintenance and downtime

The CPR 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 through news tickers in the CPR.

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 may be made pursuant to separate agreement.

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.

13 Errors and defects

In the event of errors or defects in a data delivery from the CPR, where 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.

14 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.

15 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.

16 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.

17 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 CPR data deliveries and forms or phase out service products, output media, etc. subject to reasonable notice.