OPERATIONAL CIRCULAR NO. 11
Published by the Human Resources Department

This Operational Circular was examined by the Standing Concertation Committee at its meeting on 18 October 2018.

Applicable to:
Any person working at or on behalf of CERN, as well as any other person whose Personal Data is processed by the Organization

Person responsible for the matter concerned:
Director-General

Date: January 2019

THE PROCESSING OF PERSONAL DATA AT CERN

Table of contents

I. INTRODUCTION

1. In carrying out the mission with which it is entrusted by its Member States, the Organization, as employer, host laboratory and the entity responsible for the CERN site, collects and uses Personal Data related to people who interact with CERN, including CERN "contributors" (members of the personnel, consultants, contractors working on the site, and persons engaged in any other capacity at or on behalf of CERN), the spouses and dependent children of members of the personnel, members and/or beneficiaries of the CERN Health Insurance Scheme and the CERN Pension Fund, prospective members of the personnel, suppliers and members of the public.

2. CERN is committed to respecting the security and confidentiality of the Personal Data for which it is responsible, in accordance with its Data Privacy Protection Policy[1]. Data privacy is also an integral component of the Code of Conduct[2].

3. In accordance with best practices, CERN processes only such Personal Data as is required for the proper functioning of the Organization.

II. PURPOSE AND SCOPE

4. The purpose of this Circular is to set out the Organization's approach to data privacy protection.

5. This Circular applies to all persons whose Personal Data is processed by the Organization and all persons and entities processing Personal Data on its behalf.

III. DEFINITIONS

6. **Personal Data** is any information, in any form or medium, relating to an identified or identifiable person. It includes data such as name, passport or other national registration details, CERN ID number, banking information, personnel records, images and video-surveillance footage, online and device identifiers, addresses and telephone numbers, and **Sensitive Personal Data**.

7. **Sensitive Personal Data** is any Personal Data relating to:

   7.1. physical or mental health;

   7.2. genetic or biometric data;

   7.3. racial or ethnic origin;

   7.4. sexual orientation;

   7.5. political, religious or philosophical opinions or beliefs.

8. CERN is the **Data Controller** for all processing of Personal Data falling under the scope of this Circular. As Data Controller, CERN is responsible for determining the necessary purposes and mean of processing Personal Data.

[1] Available at: https://cds.cern.ch/record/2644373
[2] Available at: https://cds.cern.ch/record/2240689

9. A **Data Subject** is any person whose Personal Data is processed by the Organization. For the purposes of this Circular, "Data Subject" includes any person authorised to act on behalf of the Data Subject concerned.

10. **Data Processing**, whether manual or automated, encompasses all activities relating to Personal Data, such as the initial collection of Personal Data, its use, retention, storage, access, display, duplication, Transfer and destruction.

11. **Anonymisation** is an irreversible process that removes any data that can be used to identify a person either directly or indirectly, rendering the Data Subject unidentifiable by the Service Owner or by third parties.

12. **Data Security** refers to the organisational, physical and technical measures put in place to safeguard the integrity of Personal Data and prevent events and activities such as unauthorised access, modification, disclosure or destruction.

13. For the purpose of this Circular, a **Service** denotes one or more activities involving the processing of Personal Data on a regular basis for the benefit of the Organization.

    13.1. **Controlling Services** determine their own purposes and means of processing Personal Data.

    13.2. **Processing Services** process Personal Data solely on behalf of Controlling Services.

14. A **Service Owner** is the person accountable for the processing of Personal Data by his or her Service.

15. A **Privacy Notice** is a published document that explains why the Organization processes Personal Data, details its Processing operations and informs Data Subjects of their rights (as set out in Section VII below).

16. A **Record of Processing Operations** details the Personal Data Processing carried out by a Controlling Service.

17. **Profiling** means any form of automated processing of Personal Data to evaluate certain aspects relating to a Data Subject, in particular, but not restricted to, his or her performance at work or behaviour.

18. A **Data Privacy Impact Assessment** is a process carried out to identify the impact on and risks of Processing operations to the rights of Data Subjects and to determine the appropriate mitigation measures.

19. **Transfer** of Personal Data occurs whenever Personal Data is shared with, or access to such Data is granted to, one or more Services or External Entities.

20. An **External Entity** is any legal person outside the Organization from which CERN receives, or to which it transfers, Personal Data.

21. **Consent** is the express, specific, informed, unambiguous and freely given permission of the Data Subject for the Processing of his or her Personal Data.

22. A **Data Breach** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

23. **Biometric Data** is Personal Data that results from specific technical processing and that relates to the physical, physiological or behavioural characteristics of a person and allow or confirm his or her unique identification.

24. **Genetic Data** is Personal Data relating to the inherited or acquired genetic characteristics of a person, which gives unique information about his or her physiology or health and which results, in particular, from an analysis of a biological sample taken from him or her.

IV. GENERAL PRINCIPLES

25. Only Services registered in the CERN Service Catalogue are authorised to process Personal Data on a regular basis. Occasional Data Processing unrelated to the specific professional activities of CERN, such as the organisation of a group social event, may be undertaken, provided that the principles set out in this Circular are respected.

26. Each Service Owner shall be responsible for his or her Service's compliance with this Circular.

27. The following key processing principles shall be observed:

    27.1. the rights of Data Subjects (as set out in Section VII below) shall be respected;

    27.2. Personal Data shall be processed in a fair and transparent manner and in accordance with CERN's internal legislation (*inter alia* the Staff Rules and Regulations, the Rules and Regulations of the Pension Fund, the Rules of the CERN Health Insurance Scheme, and Operational and Administrative Circulars);

    27.3. a purpose shall be defined for Personal Data Processing. Processing beyond such purpose, or beyond purposes closely related to the initially defined purpose, is not permitted except pursuant to paragraph 27.4 below;

    27.4. on an exceptional basis, further and/or additional processing is permitted, subject to the prior approval of the Office of Data Privacy (ODP) (see Section V below). Where prior approval is not feasible and the processing is required for the immediate functioning of the Organization or is in the vital interest of the Data Subject, such processing is permitted provided that the ODP is promptly notified;

    27.5. Personal Data Processing shall be proportionate and, as such, adequate, relevant and the minimum required to achieve the stated purpose;

    27.6. Personal Data Security measures adapted to the nature of the data concerned shall be implemented;

    27.7. Personal Data accuracy shall be ensured to the extent possible; and

    27.8. Personal Data shall be retained only for as long as is strictly necessary for the stated purpose of collection and processing.

28. The Organization shall process Personal Data only on one of the following bases:

    28.1. in order to enter into or execute a contract with the Data Subject;

    28.2. in order to apply its internal legislation and comply with its legal obligations;

    28.3. in order to pursue its legitimate interest, provided that this does not outweigh the privacy rights of the Data Subject as set out in this Circular;

    28.4. where such processing is in the vital interest of the Data Subject;

28.5. where such processing is necessary for the purposes of maintaining the Organization's archives, for scientific or historical research or for the preparation of statistics, always subject to the relevant internal legislation and policies; or

28.6. with the Consent of the Data Subject.

29. The processing of Sensitive Personal Data shall be prohibited, except in the following situations:

29.1. such processing is necessary for CERN to carry out its legal obligations, in particular in matters related to its personnel and the provision and administration of health services or social insurance;

29.2. such processing is necessary for CERN to carry out internal investigations or disciplinary procedures, or in the settlement of disputes;

29.3. such processing is necessary for the establishment, exercise or defence of legal claims;

29.4. such processing is necessary for the protection of the vital interests of the Data Subject or another person, and the Data Subject is legally or physically incapable of giving Consent;

29.5. such processing is essential for carrying out CERN's specific activities, provided that appropriate safeguards are implemented and that no less intrusive measures are reasonably available;

29.6. the Sensitive Personal Data has been manifestly made public by the Data Subject; or

29.7. the Data Subject Consents to such processing.

30. Personal Data relating to a person under 16 years of age can be processed only where absolutely necessary for the achievement of CERN's legitimate aims and as provided for in CERN's internal legal framework, or with the Consent of the person's parent or legal guardian.

31. All persons involved in Personal Data Processing shall cooperate fully in data privacy protection matters, in particular in response to specific requests from the ODP.

V. OFFICE OF DATA PRIVACY

32. The ODP shall constitute a centre of expertise for Data Subjects and for Services and External Entities involved in the Processing of Personal Data, on all issues related to the Organization's data privacy protection.

33. The ODP shall provide guidance on the implementation of the provisions of this Circular.

34. The ODP shall maintain a common interface to enable Data Subjects to exercise their rights.

35. All issues that relate to data privacy protection shall require the timely involvement of the ODP.

36. The ODP shall have access to specific Processing operations where this is essential for the purpose of its functions. Such access shall not extend to the content of the Personal Data concerned without authorisation from the Director-General.

37. The ODP shall ensure that records are maintained of advice given and of compliance checks and other relevant functions performed by the ODP, as well as of all Data Breach notifications.

38. The ODP shall be represented in a cross-disciplinary group set up by the Management of the Organization to advise on data privacy protection issues.

39. The ODP shall be headed and managed by the Data Privacy Adviser (DPA).

40. The DPA shall be appointed by the Director-General for an initial period of three years, which may be extended or renewed by the Director-General at his or her discretion.

41. The mandate of the DPA shall be approved by the Director-General and published on the ODP website.

42. The DPA shall exercise his/her functions in an independent and impartial manner. He/she shall report directly to the Director-General.

VI. OBLIGATIONS OF THE ORGANIZATION

43. As Data Controller, the Organization shall implement the appropriate technical and organisational measures needed to ensure that the processing of Personal Data is performed in accordance with this Circular.

44. The Organization shall maintain an up-to-date and publicly accessible Privacy Notice as well as an archive of all previous versions thereof.

45. The Organization shall provide relevant data privacy protection tools and training.

A. Record of Processing Operations

46. In accordance with the procedure established by the ODP, each Controlling Service shall establish one or more Records of Processing Operations relating to the Personal Data it processes.

47. The Record of Processing Operations shall contain at least all of the following information:

    47.1. the type(s) of Personal Data being processed;

    47.2. the purpose of its collection;

    47.3. the period for which it is retained;

    47.4. where applicable, details regarding use of automated decision-making; and

    47.5. where applicable, details regarding transfers of Personal Data.

48. The ODP shall ensure that the Records of Processing Operations are established and that a complete archive of such Records is maintained.

49. In the event of a change in the manner in which a Controlling Service processes Personal Data, the Service shall update its Record of Processing Operations accordingly and shall archive all previous versions.

    49.1. If the change could reasonably be considered as having a significant impact on the rights of Data Subjects (as set out in Section VII below), the Service shall obtain advice from the ODP on, *inter alia*, the additional notification requirements.

49.2. If the change concerns Personal Data that is processed on a Consent basis, the Service shall individually notify each affected Data Subject of the updated Record of Processing Operations and shall obtain his or her ongoing Consent to processing.

B. Accuracy and relevance

50. Each Service shall take reasonable measures to correct or delete Personal Data that is inaccurate, excessive or unnecessary.

51. Each Service shall make reasonable efforts to notify other Services, as well as External Entities to which the Personal Data has been transferred, of any such measures taken and shall request that they undertake similar remedial action.

C. Data retention

52. The ODP shall issue retention period guidelines in order to ensure consistency throughout the Organization.

53. Each Controlling Service shall establish its own data retention periods on the basis of these guidelines, taking due account of:

53.1. the general purpose of the processing of the Personal Data in question;

53.2. how long the Personal Data is reasonably required to be kept in order to fulfil such purpose;

53.3. the impact of the retention period on the rights of Data Subjects (as set out in Section VII below);

53.4. financial and organisational costs, risks of breach and risks of unlawful Processing, as well as liabilities associated with the retention of the Personal Data; and

53.5. measures needed to ensure that the Personal Data is kept up-to-date.

54. At the end of the retention period, or earlier if the purpose of its processing has been fulfilled, each Controlling Service shall destroy or anonymise Personal Data, as appropriate. Should this not prove possible, it shall put safeguards in place to prevent any continued or future processing.

D. Data Security

55. The Organization shall periodically evaluate the effectiveness of its Data Security measures.

E. Data Privacy Impact Assessment

56. Each Controlling Service shall undertake a Data Privacy Impact Assessment, in accordance with the procedure established by the ODP, prior to undertaking any Processing operation that has one or more of the following characteristics:

56.1. includes Sensitive Personal Data;

56.2. poses a high risk to the rights of Data Subjects (as set out in Section VII below);

56.3. involves a significant technological change in the processing; or,

56.4. results in large-scale or recurrent processing.

57. The Service Owner shall determine whether a Data Privacy Impact Assessment is required; if in doubt, he or she shall consult the ODP.

58. A single assessment can be carried out for multiple Processing operations that pose similar risks.

59. Data Privacy Impact Assessments shall be sent to the ODP, which will maintain a record of the assessments carried out. Where the ODP considers that the proposed Processing operation is not proportionate to its stated purpose, it shall recommend how best to adapt the Processing operation. Where such adaptation is not feasible, the ODP can request that the Processing operation not be undertaken.

F. Privacy by design

60. Processing operations shall be designed and implemented in accordance with this Circular.

61. Service Owners shall keep detailed records of the privacy considerations that have been taken into account in the conception and design of the Processing operations.

G. Data Breach

62. In the event of a Breach in Data Security resulting in, *inter alia*, the improper access to or use, alteration, destruction, loss or transfer of Personal Data, the Service shall trigger the Organization's Data Breach response procedure.

63. Each Data Subject shall be notified of any Breach concerning his or her own Sensitive Personal Data.

64. Insofar as other Personal Data is concerned, each Data Subject shall be notified of any Breach that results in a high and unavoidable risk to his or her rights (as set out in Section VII below), where such notification does not involve disproportionate efforts.

65. This notification shall be established in accordance with advice provided by the ODP.

VII. RIGHTS OF DATA SUBJECTS

66. Information on how to exercise the rights set out in Sub-sections A to J below is published[3] by the Organization in its Privacy Notice.

A. Right to information

67. Each Data Subject shall have access to information on data privacy protection at CERN.

B. Right to access

68. Each Data Subject is entitled to:

68.1. enquire about the legal basis and purpose underlying the processing of his or her Personal Data;

[3] For instance, on the website of the ODP.

68.2. request a copy of his or her Personal Data upon submission of an access request; and

68.3. enquire whether his or her Personal Data has been or is to be transferred to an External Entity, as well as about the safeguards taken.

C. Right to object

69. Each Data Subject is entitled to challenge the legitimacy of the Organization's processing of his/her Personal Data where he or she is able to demonstrate compelling reasons.

D. Right to correction

70. Each Data Subject is entitled to request the prompt correction of his or her Personal Data, where he or she is able to demonstrate that the data is inaccurate or incomplete.

71. The ODP shall ensure that the Data Subject is notified of any measures taken in response to a request submitted under paragraph 70 and that reasonable efforts are made to notify any Services or External Entities acting as Controllers to which the Personal Data has been transferred and to request that said Controllers undertake similar measures.

E. Right to request temporary suspension of processing

72. Each Data Subject is entitled to request the temporary suspension of the processing of his/her Personal Data for specified purposes where:

72.1. he or she demonstrates that the data is inaccurate and seeks suspension until such time as correction or deletion can be effectively done; or

72.2. it is no longer necessary for CERN to Process the data but the data is required by the Data Subject for the establishment, exercise or defence of legal claims (*e.g.* the Data Subject may ask the Service to refrain from deleting his or her data).

73. Upon receipt of a reasonable request for the suspension of processing, and pending a decision in respect of such request, the Organization shall promptly refrain from any non-essential processing of the Personal Data in question.

74. The ODP shall ensure that the Data Subject is notified of any measures taken in response to a request submitted in accordance with paragraph 72. If the request for suspension of processing is granted, the Data Subject shall also be informed of any subsequent decision to lift the suspension and to resume the processing of his or her Personal Data.

F. Right to deletion

75. Subject to the provisions of Sub-section J below, each Data Subject is entitled to request the deletion of his or her Personal Data if:

75.1. the Data was not collected in compliance with this Circular;

75.2. the Data is processed on the basis of Consent, and the said Consent has been withdrawn; or

75.3. the processing of his/her Personal Data is no longer necessary for the stated purpose for which it was collected and processed.

76. The ODP shall ensure that the Data Subject is notified of any measures taken in response to a request submitted in accordance with paragraph 75 and that reasonable efforts are made to notify Services or any External Entities to which the Personal Data has been transferred of such measures.

G. Right to portability

77. Each Data Subject is entitled to promptly receive his or her Personal Data in a reasonable and reusable format, where:

77.1. the Data was collected on the basis of Consent or contract; and

77.2. the data exists in a digital format.

78. At the discretion of the Director-General, a portability request may be granted even where it does not meet the conditions provided for in paragraph 77.

H. Rights in respect of automated decision-making

79. Each Data Subject is entitled to be informed of automated decision-making, including Profiling, that affects him or her.

80. He or she is entitled to express his or her views and have them taken into consideration where such automated decision-making significantly affects him or her.

I. Conditions governing the exercise of the rights

81. Each Data Subject wishing to exercise the rights set out in Sub-sections A to H above shall submit a request via the common interface established by the ODP.

82. The Data Subject shall be required to prove his or her identity. CERN is entitled to ask for such information as it deems necessary in this regard.

83. The Organization has the discretion to deny a request if it deems it to be unreasonable, manifestly abusive, fraudulent or obstructive to the purpose of the processing (*e.g.* due to its repetitive or unduly broad nature) or if granting the request would involve a disproportionate effort or violate the rights of other Data Subjects.

84. The Data Subject shall be entitled to receive a written response to his or her request, including the reasons for the decision, within 90 calendar days.

85. If the Data Subject is not satisfied with the Organization's response, he or she is entitled to exercise recourse to the report and/or complaint mechanisms set out in Section IX.

J. Restrictions

86. The rights set out in Sub-Sections A to H above may be restricted by the Director-General, at his or her discretion, on a temporary, exceptional and specific basis, where:

86.1. such restriction is necessary for the prevention, detection or investigation of possible misconduct or illegal activity;

86.2. CERN has received a request for the Transfer of Personal Data from national authorities, and the request is reasonable and compatible with the status of the Organization; or

86.3. such restriction is essential to safeguard the rights, safety and security of the Data Subject or of other individuals or the security of the Organization's premises or its functioning.

87. Wherever possible, any such decision by the Director-General shall promptly be made available, in writing, to the affected Data Subject(s).

VIII. TRANSFERS

A. Transfers within CERN

88. Personal Data shall be transferred between Services only for such purposes as are stated in their respective Records of Processing Operations.

89. Controlling Services shall inform other Services to which they transfer Personal Data of the Transfer to enable the latter to ensure that the appropriate organisational and technical measures are applied.

90. Notwithstanding the foregoing, Services may transfer Personal Data to other Services where they have determined that this would be in the interest of the Organization and the ODP has approved the Transfer. The ODP may recommend that additional safeguards be put in place.

B. Transfers between CERN and External Entities

91. Where CERN receives Personal Data from an External Entity, the Organization shall, prior to any processing occurring at or on behalf of CERN, verify that the Transferring Entity was legally entitled to transfer such data.

92. Prior to transferring Personal Data to an External Entity, the transferring Service shall ensure that the recipient has been instructed that Personal Data must be processed lawfully and in accordance with the principles set out in the present Circular. Onward Transfers from the External Entity shall be subject to the same obligations.

93. The Transfer of Sensitive Personal Data to an External Entity is prohibited, unless the ODP has been consulted and:

93.1. the Data Subject has explicitly given Consent to such Transfer, or it is in his or her vital interests;

93.2. the Transfer is essential to the operations of CERN, e.g. for health, safety, residency or employment purposes; or

93.3. The Transfer is formally requested by a national or intergovernmental entity in the context of such purposes as public health, administration of justice or national security, and the request has been deemed by the Director-General to be both reasonable and compatible with the status of the Organization.

94. The Data Subject shall be informed of the Transfer of his or her Personal Data to an External Entity, except in the context of paragraph 93.3 or where the Organization has a compelling reason not to so notify.

C. Processing by External Entities

95. When processing of Personal Data is carried out by an External Entity for or on behalf of CERN, the Organization shall require that such entity complies with the principles set out in this Circular and that appropriate safeguards are in place to protect the privacy of the Data Subjects concerned.

IX. REPORT AND COMPLAINT MECHANISMS

96. The Organization has a two-tier system allowing it to respond to concerns that Personal Data has been processed in a manner that is not compliant with this Circular: an informal report mechanism and a formal complaint mechanism.

97. A report or complaint that is frivolous, manifestly unfounded or made in bad faith may be immediately dismissed and may result in administrative and/or disciplinary action.

A. Report mechanism

98. All persons with knowledge of the misprocessing, or the potential for misprocessing, of Personal Data shall file a report with the ODP.

99. The ODP shall evaluate the report and, where it deems appropriate, shall inform the Service(s) involved of any recommended remedial action and/or advise any Data Subject(s) concerned of their right to lodge a formal complaint.

B. Complaint mechanism

100. A Data Subject who has not achieved satisfaction after a report has been filed with the ODP with respect to the Processing of his or her Personal Data may file a formal complaint in accordance with the Organization's procedures.

X. IMPLEMENTATION

101. The Organization shall implement this Circular in accordance with a staged schedule approved by the Director-General and published on the website of the ODP.

*****