Ordinance to the Federal Act on Data Protection (DPO)

(Preliminary draft, published on 23 June 2021)

Unofficial English translation done in summer 2021

The officials versions, in German, French and Italian, will be published on https://www.fedlex.admin.ch/de/, and will be the only legally binding versions.

Ordinance to the Federal Act on Data Protection (DPO)

PRELIMINARY DRAFT

The Swiss Federal Council,

based on Articles 8(3), 10(4), 12(5), 16(3), 25(6), 28(3), 33, 59(2) and (3) of the Federal Act of 25 September 2020[1] on Data Protection (FADP),
ordains:

Chapter 1 General Provisions
Section 1 Data Security

Art. 1 Principles

[1] Whether the technical or organisational measures to ensure data security are appropriate to the risk is assessed according to the following criteria:

a. The purpose, nature, extent and circumstances of the data processing;
b. the likelihood of occurrence of a data breach and its potential impact on data subjects;
c. the state of the art;
d. costs of implementation.

[2] The measures shall be reviewed at appropriate intervals throughout the processing period.

Art. 2 Protection objectives

As far as appropriate, the measures to ensure data security must achieve the following protection objectives:

a. Access control: access by authorised persons must be limited to the personal data that they require to fulfil their task.
b. Entrance control: unauthorised persons must be denied access to the facilities and installations in which personal data is being processed.
c. Data carrier control: it must not be possible for unauthorised persons to read, copy, alter, move or remove data carriers.
d. Storage control: unauthorised storage in the data memory as well as unauthorised knowledge, alteration or deletion of stored personal data must be prevented.
e. Usage control: the use by unauthorised persons of automated data processing systems by means of devices for data transmission must be prevented.
f. Transport control: when disclosing personal data as well as during the transport of data carriers, the unauthorised reading, copying, alteration or deletion of data must be prevented.
g. Input control: in automated systems, it is possible to carry out an examination of what personal data was entered or altered at what time and by which person.
h. Disclosure control: it is possible to check to whom personal data has been disclosed by means of devices for data transmission.
i. Recovery: the availability of and access to personal data can be rapidly restored in the event of a physical or technical incident.
j. It is ensured that all functions of the system are available (availability), that malfunctions are reported (reliability) and that stored personal data cannot be damaged by system malfunctions (data integrity).

1 SR **235.1**

k. Detection: data security breaches can be quickly detected, and measures can be taken to mitigate or eliminate the impact.

Art. 3 Records

[1] If the data protection impact assessment shows that during the automated processing of personal data there is still a high risk to the personality or fundamental rights of data subjects despite the measures provided by the controller, the private controller and its processor shall record at least the following processes: the storage, alteration, reading, disclosure, deletion or destruction of data.
[2] Federal bodies and their processors shall record at least the following processes during the automated processing of personal data: the storage, alteration, reading, disclosure, deletion or destruction of data.
[3] The records provide information on the nature of the processing operation, the identity of the person who carried out the processing, the identity of the recipient and the time at which the processing took place.
[4] The records must be kept for two years separately from the system in which the personal data is being processed. They must be accessible only to the bodies or persons responsible for monitoring data protection provisions or for restoring the confidentiality, integrity, availability and traceability of the data, and may only be used for this purpose.

Art. 4 Processing policy for private persons

[1]The controller and its processor must draw up a processing policy for automated processing if they:
a. process sensitive personal data on a broad scale; or
b. carry out high-risk profiling.

[2] The policy must at least contain information on:

a. the purpose of processing;
b. the categories of data subjects and the categories of personal data processed;
c. the retention period of the personal data or the criteria for determining this period;
d. the internal organisation;
e. the origin of the personal data and the way in which it was collected;
f. the technical and organisational measures taken to ensure data security;
g. the access authorisations and the nature and extent of access;
h. the measures taken to minimise data;
i. the data processing procedures, in particular the procedures for the storage, correction, disclosure, retention, archiving, pseudonymisation, anonymisation and deletion or destruction of data;
j. the procedure for exercising the access right and the right of data portability.

[3] The private person must update the processing policy regularly and make it available to the data protection advisor in a form that is comprehensible to the advisor.

Art. 5 Processing for federal bodies

[1]The federal body responsible and its processor shall draw up a processing policy for automated processing if they:
a. process sensitive personal data;
b. carry out a profiling;
c. carry out data processing activities in accordance with Article 34(2)(c) FADP;
d. make personal data accessible to cantons, foreign authorities, international organisations or private persons;
e. interlink data files; or
f. operate an information system in conjunction with other federal bodies or manage data files.

[2] The processing policy must at least contain the information specified in Article 4(2).

[3] The federal body responsible must update the processing policy regularly and make it available to the data protection advisor in a form that is comprehensible to the advisor, and to the Federal Data Protection and Information Commissioner (FDPIC) on request.

Section 2 Data Processing by Processors

Art. 6 Modalities

[1]The controller who assigns the processing of personal data to a processor remains responsible for data protection matters. The controller must ensure that the data is being processed in accordance with a contract or the law.

[2]If the processor is not subject to the FADP, the controller must ensure that other legal provisions guarantee an equivalent level of data protection. Otherwise the controller must ensure data protection by contractual means.[3] Personal data may only be collected for a specific purpose which is evident to the data subject; personal data may only be processed in a way that is compatible with such purpose.

[3]If the controller is a federal body, the processor may assign data processing to a third party if the federal body has consented thereto in writing.

Art. 7 Information to the data protection advisor of the federal body

The federal body shall inform the data protection advisor without delay of the conclusion of a contract with a processor or the authorisation to transfer data processing to a third party. The federal body shall also inform the data protection advisor if problems arise in complying with the statutory or contractual data protection provisions.

Section 3 Cross-Border Disclosure of Personal Data

Art. 8 Assessment of the adequacy of the level of data protection of a foreign State or an international body

[1] If personal data is disclosed abroad, the assessment of whether a State, a territory, one or more specific sectors in a State or an international body ensures an adequate level of data protection must be based on the following criteria:

a. the international obligations of the State or international body with respect to data protection;
b. respect for human rights;
c. the applicable legislation on data protection and its implementation, and the relevant case law;
d. the effective guarantee of the rights of data subjects and of judicial protection;
e. the effective functioning of one or more independent authorities responsible for data protection matters in the State concerned or to which an international body is answerable, and which have sufficient powers and competences.

[2] The assessment may take into account the evaluations of international bodies or foreign authorities responsible for data protection matters.

[3] The adequacy of the level of data protection of the State, territory, specific sectors in a State or the international body shall be reassessed periodically.

[4] If an assessment under paragraph 3 or available information indicates that a State, a territory, one or more specific sectors in a State or an international body no longer ensures an adequate level of data protection, the decision in accordance with Article 16(1) FADP shall be amended, stayed or revoked. This new decision has no effect on data disclosures made prior thereto.

[5] The States, territories, specific sectors in a State and international bodies with an adequate level of data protection are listed in Annex 1.

[6] The FDPIC shall be consulted prior to any decision on the adequacy of the level of data protection.

Art. 9 Data protection provisions and specific safeguards

[1]The data protection provisions of a contract in accordance with Article 16(2)(b) FADP and the specific safeguards in accordance with Article 16(2)(c) FADP must at least regulate the following aspects:

a. the application of the principles of lawfulness, good faith, proportionality, purpose limitation and accuracy;

b. the categories of personal data disclosed as well as the data subjects;
c. the nature and purpose of the disclosure of personal data;
d. the names of the States to which personal data is disclosed;
e. the names of the international bodies to which personal data is disclosed;
f. the requirements for the retention, deletion and destruction of personal data;
g. the recipients authorised to process the data;
h. the measures to ensure data security;
i. the requirements for the disclosure of personal data to another foreign State or to another international body;
j. the duty of the recipient to inform the data subjects of the processing;
k. the rights of the data subjects, in particular:
    1. access right,
    2. right to object to processing of personal data,
    3. right to correction, deletion or destruction of personal data,
    4. right to seek judicial protection from an independent authority.

[2] The controller must take appropriate measures to ensure that the recipient complies with the data protection provisions of a contract or the specific safeguards.

[3] If the FDPIC has been informed of the data protection provisions of a contract or the specific safeguards, the duty of information shall be deemed to be fulfilled for all further disclosures that:

a. are made subject to the same data protection provisions or safeguards, provided the categories of recipients, the purpose of the processing and the data categories remain essentially unchanged; or
b. take place within the same legal person or company or between legal persons or companies belonging to the same group, provided that the data protection provisions or safeguards continue to ensure an adequate level of data protection.

Art. 10 Standard data protection clauses

[1] If the controller discloses personal data abroad by means of standard data protection clauses in accordance with Article 16(2)(d) FADP, the controller shall take appropriate measures to ensure that the recipient complies therewith.

[2] The FDPIC has published a list of standard data protection clauses that he has approved, established or recognised.

Art. 11 Binding corporate rules on data protection

[1] Binding corporate rules on data protection in accordance with Article 16(2)(e) FADP apply to all companies belonging to the same group.

[2] They shall at least contain the aspects mentioned in Article 9(1) as well as the following information:

a. the organisation and contact details of the group and its companies;
b. the measures taken within the group to ensure compliance with the binding corporate rules on data protection.

Art. 12 Codes of conduct and certifications

[1] Personal data may be disclosed abroad if an adequate level of data protection is ensured by a code of conduct or certification.

[2] The code of conduct shall at least contain the information specified in Article 9(1) and must be approved in advance by the FDPIC.:

[3] The code of conduct or certification must be linked to a binding and enforceable obligation on the part of the controller or the processor in the third country to apply the measures contained therein.

Chapter 2 Duties of the Controller and the Processor

Art. 13 Modalities of the duties of information

[1] The controller and the processor shall communicate the information on the collection of personal data in a precise, comprehensible and easily accessible form.

[2] If the information is provided in combination with pictograms that are displayed electronically, they must be machine-readable.

Art. 14 Duty of information of federal bodies in the case of systematic collection of personal data

Where a federal body collects personal data systematically, in particular by means of questionnaires, the federal body responsible must inform data subjects who are not obliged to provide information that the provision of information is voluntary.

Art. 15 Information on the disclosure of personal data

The controller and the processor shall notify the recipient of the up-to-dateness, reliability and completeness of the personal data that they disclose, provided this information is not evident from the data itself or from the circumstances.

Art. 16 Information on the correction, deletion or destruction as well as the restriction of processing of personal data

The controller shall inform the recipients to whom it has disclosed personal data without delay of the correction, deletion or destruction as well as the restriction of the processing of personal data, unless notification is impossible or involves a disproportionate effort.

Art. 17 Review of an automated individual decision

Where a data subject of an automated individual decision requests that he or she be able to state his or her position or for a natural person to review the decision, the data subject must not be disadvantaged as a result.

Art. 18 Form and retention of data protection impact assessment

The controller must record the data protection impact assessment in writing. It must be retained for two years after termination of the data processing activity.

Art. 19 Notification of data security breaches

[1] The controller shall notify the FDPIC in the event of a data security breach of:

a. the nature of the data security breach;
b. as far as possible, the time and duration of the data security breach;
c. as far as possible, the categories and approximate number of personal data concerned;
d. as far as possible, the categories and approximate number of data subjects;
e. the impact, including any risks, for the data subjects;
f. what measures have been taken or are envisaged to remedy the defect or mitigate the impact;
g. the name and contact details of a contact person.

[2] If, upon discovery of the data security breach, the controller is unable to provide the FDPIC with all the information specified in paragraph 1 at the same time, it may provide this information step by step without undue further delay.

[3] The controller shall inform the data subjects in simple and comprehensible language of at least the information referred to in paragraph 1 letters a, e, f and g.

[4] If the controller is a federal body, the notification to the FDPIC shall be made via the data protection advisor.

[5] The controller must document data security breaches. The documentation must contain all facts relating to the incidents, their effects and the measures taken. The documentation must be retained for at least three years from the date of notification according to paragraph 1.

Chapter 3 Rights of the Data Subject

Section 1 Access Right

Art. 20 Modalities

[1] The information request shall be made in writing. If the controller agrees, the request may also be made verbally.

[2] As a rule, the information shall be provided in writing. With the agreement of the controller or at its suggestion, the data subject may also inspect his or her data in situ. The information may also be provided verbally if the data subject has consented thereto.

[3] The information must be comprehensible to the data subject.

[4] The controller must take appropriate measures to ensure identification of the data subject and to protect the data subject's personal data from access by unauthorised third parties when providing information. Data subjects must cooperate in their identification.

[5] The controller shall document the grounds on which it refuses, restricts or defers the provision of the information. The documentation shall be retained for at least three years.

Art. 21 Responsibilities

[1] If several controllers are responsible for the processing of personal data, the data subject may assert his or her access right against each controller. If a controller is not competent for dealing with the information request, it shall pass the request on to the competent controller.

[2] If the information request relates to data that is being processed by a processor, the controller shall pass the request on to the processor if the controller is not able to provide the information itself.

Art. 22 Time limits

[1] The information is provided within 30 days of receipt of the information request. If the controller refuses, restricts or defers the provision of the information, it must notify the data subject thereof within the same period.

[2] If the information cannot be provided within 30 days, the controller must notify the data subject thereof and of the date by which the information will be provided.

Art. 23 Exceptions to the exemption from costs

[1] The payment of an appropriate share of the costs may be requested if the provision of information involves a disproportionate effort.

[2] The share of the costs amounts to a maximum of 300 Swiss Francs.

[3] The data subject must be notified of the amount of the share before the information is provided and may withdraw his or her request within ten days.

Section 2 Right of Data Portability

Art. 24

Articles 20(1), (4) and (5), and 21, 22 and 23 shall apply mutatis mutandis to the right of data portability and its restrictions.

Chapter 4 Special Provisions for Data Processing by Private Persons

Art. 25 Data protection advisor

[1] The data protection advisor of a private controller must perform the following duties:

a. The data protection advisor audits the processing of personal data as well as its prerequisites and recommends corrective measures if he or she ascertains that the data protection regulations have been infringed.
b. The data protection advisor participates in the preparation of the data protection impact assessment and reviews it, at any rate if the private controller wishes to abstain from consulting the FDPIC in accordance with Article 23(4) FADP.

[2] The private controller must provide the data protection advisor with:

a. the necessary resources;
b. access to all information, documents, inventories of processing activities and personal data that the data protection advisor requires in order to fulfil his or her duties.

Art. 26 Exemptions from the duty to keep an inventory of processing activities

Companies and other organisations under private law which employ fewer than 250 members of staff at the beginning of a year, as well as natural persons, are exempt from the duty to keep an inventory of processing activities, unless one of the following conditions is met:

a. Sensitive personal data is being processed on a broad scale.
b. High-risk profiling is carried out.

Chapter 5 Special Provisions for Data Processing by Federal Bodies

Section 1 Data Protection Advisor

Art. 27 Appointment

Each federal body appoints a data protection advisor. Several federal bodies may jointly appoint a data protection advisor.

Art. 28 Requirements and duties

[1] The data protection advisor must meet the following requirements:

a. The data protection advisor has the necessary professional knowledge.
b. The data protection advisor performs his or her function towards the federal body in a professionally independent manner and without being bound by instructions.

[2] The data protection advisor must perform the following duties:

a. The data protection advisor audits the processing of personal data as well as its prerequisites and recommends corrective measures if he or she ascertains that the data protection regulations have been infringed.
b. The data protection advisor participates in the preparation of the data protection impact assessment and reviews it.
c. The data protection advisor reports data security breaches to the FDPIC.
d. The data protection advisor serves as a contact point for data subjects.
e. The data protection advisor trains and advises the federal body and its members of staff on data protection matters.

Art. 29 Duties of the federal body

[1] The federal body shall grant the data protection advisor access to all information, documents, inventories of processing activities and personal data that the data protection advisor requires in order to fulfil his or her duties.

[2] The federal body publishes the contact details of the data protection advisor on the internet and communicates them to the FDPIC.

Art. 30 Contact point of the FDPIC

The data protection advisor serves as a contact point for the FDPIC for questions relating to the processing of personal data by the federal body concerned.

Section 2 Projects of Federal Bodies Involving Automated Processing of Personal Data

Art. 31 Information to the data protection advisor

The federal body responsible shall inform the data protection advisor in good time when planning a project involving the automated processing of personal data as well as in the event of adjustments after project completion so that data protection requirements are taken into account without delay.

Art. 32 Notification to the FDPIC

[1] The federal body responsible shall notify the FDPIC of the planned automated processing activities at the time of the project approval or the decision on the development of the project. The FDPIC shall include this notification in its register on processing activities.

[2] The notification must include the information specified in Article 12(2)(a-d) FADP and the expected date of commencement of the processing activities.

[3] The federal body responsible shall update the notification at the time of the transition into productive operation or when the project is discontinued.

Section 3 Pilot Projects

Art. 33 Indispensability of test phase

A test phase as a pilot project is indispensable if one of the following conditions is met:

a. The fulfilment of a task requires technical innovations, the effects of which must first be evaluated.
b. The fulfilment of a task requires significant organisational or technical measures, the effectiveness of which must first be evaluated, in particular in the case of cooperation between federal and cantonal bodies.
c. The fulfilment of tasks requires that personal data be made accessible by means of a retrieval procedure.

Art. 34 Authorisation

[1] Before consulting the interested administrative units, the federal body responsible for the pilot project shall inform the FDPIC as to how it is intended to ensure compliance with the requirements of Article 35 FADP, and invite him to comment thereon.

[2] The FDPIC shall comment on the issue of whether the authorisation requirements in terms of Article 35 FADP are fulfilled. The competent federal body shall provide him with all the documents required, and in particular with:

a. a general description of the pilot project;

b. a report that proves that the fulfilment of tasks provided for by law requires the processing in accordance with Article 34(2) FADP and that a test phase before a formal law enters into force is indispensable (Article 35(1)(c) FADP);
c. a description of the internal organisation as well as the data processing and control procedures;
d. a description of the security and data protection measures;
e. the draft of or the concept for an ordinance that regulates the details of the processing;
f. information relating to the planning of the various phases of the pilot project.

3 The FDPIC may request further documents and carry out additional investigations.

4 The competent federal body shall inform the FDPIC of any important modification relating to compliance with the requirements of Article 35 FADP. If required, the FDPIC shall again state his views thereon.

5 The opinion of the FDPIC must be included in the application to the Federal Council.

6 The modalities of automated data processing are regulated in an ordinance.

Art. 35 Evaluation report

The competent federal body shall submit the draft of the evaluation report for the Federal Council to the FDPIC for comment. The Federal Council must be informed of the opinion of the FDPIC.

Section 4 Data Processing for Research, Planning and Statistics

Art. 36

If personal data is processed for purposes not related to specific persons, in particular research, planning and statistics, and at the same time for another purpose, the exceptions under Article 39(2) FADP are only applicable to processing for the purposes not related to specific persons.

Chapter 6 Federal Data Protection and Information Commissioner

Art. 37 Headquarters and permanent secretariat

1 The FDPIC's headquarters are located in Bern.

2 The employment of the members of the FDPIC's permanent secretariat is governed by the Federal Personnel Act. The employees of the FDPIC's permanent secretariat are insured against the economic consequences of old age, disability and death with the Federal Pension Fund PUBLICA.

Art. 38 Communication channel

1 The FDPIC deals with the Federal Council via the Federal Chancellor. The Federal Chancellor shall pass on any proposals, opinions and reports from the FDPIC unchanged to the Federal Council.

2 The FDPIC submits reports to the Federal Assembly via the Parliamentary Services.

Art. 39 Notification of guidelines and decisions

1 The departments and the Federal Chancellery notify the FDPIC of their data protection guidelines as well as their data protection decisions in anonymised form.

2 The federal bodies shall submit to the FDPIC any draft legislation that relates to the processing of personal data, data protection or access to official documents.

Art. 40 Processing of personal data

The FDPIC processes personal data, including sensitive personal data, in particular for the following purposes:

a. to carry out his supervisory activities;
b. to investigate breaches of data protection regulations;
c. to train and advise federal bodies and private persons;
d. to cooperate with federal, cantonal and foreign authorities;
e. to conduct mediation proceedings and evaluations in accordance with the Federal Act of 17 December 20042 on Freedom of Information in the Administration (Freedom of Information Act);
f. to respond to citizens' enquiries.

Art. 41 Self-regulation

1 The FDPIC draws up a processing policy for all automated processing activities. Article 5(1) shall not apply.

2 The FDPIC provides for internal processes to ensure that processing activities are carried out in accordance with the processing policy. He shall review annually whether the processing policy is being complied with.

Art. 42 Cooperation with the National Cyber Security Centre (NCSC)

1 The FDPIC may pass on the information on the notification of a data breach to the NCSC for analysis of the incident. The FDPIC must obtain the prior consent of the controller that is subject to the notification duty.

2 The FDPIC shall invite the NCSC to submit its comments before taking any measure towards a federal body concerning data security under Article 51(3)(b) FADP.

Art. 43 Register on processing activities of federal bodies

1 The register on the processing activities of federal bodies contains the information provided by the federal bodies and their processors according to Article 12(2) and (3) FADP and Article 32(2) of this Ordinance.

2 The register is published on the internet. The register entries on planned automated processing activities in accordance with Article 32 shall not be published.

Art. 44 Codes of conduct

If a code of conduct is submitted to the FDPIC, he shall state in his opinion whether the code of conduct meets the requirements of Article 22(5)(a) and (b) FADP.

Art. 45 Fees

1 The fees charged by the FDPIC are based on the time spent.

2 An hourly rate of 150 to 350 Swiss Francs applies. The respective rate is based on the complexity of the matter and the function of the person responsible for handling the matter.

3 In all other respects, the General Fees Ordinance of 8 September 20043 applies.

2 SR **152.3**
3 SR **172.041.1**

Chapter 7 Final Provisions

Art. 46 Repeal and amendments of other legislation

The repeal and the amendments of other legislation are set forth in Annex 2.

Art. 47 Transitional provisions concerning notification to the FDPIC of planned automated processing activities

Article 32 does not apply to planned automated processing activities for which, at the time of entry into force, the project has already been approved or the decision on development of the project has already been made.

Art. 48 Entry into force

This Ordinance comes into force on …

On behalf of the Swiss Federal Council
The President of the Confederation: Guy Parmelin
The Federal Chancellor: Walter Thurnherr

Annex 1
(Article 8(5))

States, territories, specific sectors in a State and international bodies with an adequate level of data protection

Andorra
Argentina
Austria
Belgium
Bulgaria
Canada[4]
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Faroe Islands
Finland
France
Germany
Gibraltar
Greece
Guernsey
Hungary
Iceland
Ireland
Isle of Man
Israel
Italy
Jersey
Latvia
Liechtenstein
Lithuania
Luxembourg
Malta
Monaco
New Zealand
Netherlands
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Uruguay
United Kingdom[5]

4 An adequate level of data protection is ensured when the Canadian federal law in the private sphere (The Personal Information Protection and Electronic Documents Act) or a provincial law applies that is broadly equivalent to the federal law. The Canadian federal law applies to personal data that is collected, processed or disclosed in the context of commercial activities, irrespective of whether this is done by organisations (e.g. associations, partnerships, individuals and trade unions) or federally regulated entities (facilities, plants, undertakings or business activities that fall within the legislative jurisdiction of the Canadian Parliament). The following provinces have enacted legislation that is broadly equivalent to the federal law: Québec, British Columbia and Alberta, as well as Ontario, New Brunswick, Newfoundland and Labrador and Nova Scotia (for health data). However, even in these provinces, the federal law applies, as it does in the rest of Canada, to all personal data collected, processed or disclosed by federally regulated entities, including employee data of those entities. The federal law also applies to personal data transferred to another province or country in the course of commercial activities.

5 The Federal Council's decision only relates to data processing that does not fall within the scope of the Schengen relevant Directive (EU) 2016/680. In the areas covered by Directive (EU) 2016/680, the legislation of the United Kingdom in accordance with the Commission Implementing Decision of ... pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequacy of the protection of personal data in the United Kingdom is recognised as adequate.

walderwyss

Contacts

Jürg Schneider
Dr. iur., Attorney at Law
Partner
Direct phone: +41 58 658 55 71
juerg.schneider@walderwyss.com

David Vasella
Dr. iur., Attorney at Law
Partner
Direct phone: +41 58 658 52 87
david.vasella@walderwyss.com

Hugh Reeves
MLaw, LL.M., Attorney at Law
Direct phone: +41 58 658 52 73
hugh.reeves@walderwyss.com

Attorneys at Law

Walder Wyss Ltd.
Phone +41 44 498 98 98
Fax +41 44 498 98 99
reception@walderwyss.com
www.walderwyss.com
Zurich, Geneva, Basel, Berne, Lausanne, Lugano