
**Information technology — Personal
identification — ISO-compliant driving
licence**

**Part 2:
Machine-readable technologies**

iTeh STANDARD PREVIEW
*Technologies de l'information — Identification des personnes — Permis
de conduire conforme à l'ISO
(standards.iteh.ai)
Partie 2: Technologies lisibles par une machine*

ISO/IEC 18013-2:2008

<https://standards.iteh.ai/catalog/standards/sist/6458f7c4-99d9-4490-9fb1-1b658ec0e8f1/iso-iec-18013-2-2008>

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 18013-2:2008](https://standards.iteh.ai/catalog/standards/sist/6458f7c4-99d9-4490-9fb1-1b658ec0e8f1/iso-iec-18013-2-2008)

<https://standards.iteh.ai/catalog/standards/sist/6458f7c4-99d9-4490-9fb1-1b658ec0e8f1/iso-iec-18013-2-2008>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Conformance	1
3 Normative references	2
4 Terms, definitions and abbreviations.....	2
5 Machine-readable functionality of IDLs	5
5.1 General principles	5
5.2 Mandatory functions	6
5.3 Optional functions.....	6
6 Machine-readable technologies supported	6
7 Organization of data	7
7.1 Mandatory data	7
7.2 Optional data.....	7
8 Data structure	7
8.1 Data Group 1: Mandatory text data elements.....	8
8.2 Data Group 2: Optional licence holder details	9
8.3 Data Group 3: Optional issuing authority details	10
8.4 Data Group 4: Optional portrait image	10
8.5 Data Group 5: Optional signature / usual mark image	11
8.6 Data groups 6, 7, 8 and 9: Optional facial, fingerprint, iris and other biometric templates.....	11
8.7 Data Group 10: Reserved for future use	13
8.8 Data Group 11: Optional domestic data.....	13
9 Application identifiers.....	14
Annex A (normative) Assembly rules for categories of vehicles/restrictions/conditions field.....	15
Annex B (normative) Compact encoding	26
Annex C (normative) Standard encoding for ICCs with contacts and for PICCs.....	38
Annex D (normative) Standard Encoding for Optical Memory Cards	71
Annex E (normative) Images	80
Bibliography.....	88

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18013-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

ISO/IEC 18013 consists of the following parts, under the general title *Information technology — Personal identification — ISO-compliant driving licence*:

- *Part 1: Physical characteristics and basic data set*. Part 1 defines the basic terms for ISO/IEC 18013, including physical characteristics, basic data element set, visual layout, and physical security features.
- *Part 2: Machine-readable technologies*. Part 2 defines the technologies that may be used for ISO/IEC 18013, including the logical data structure and data mapping for each technology.
- *Part 3: Access control, authentication and integrity validation*. Part 3 defines the electronic security features that may be incorporated under ISO/IEC 18013, including mechanisms for controlling access to data, verifying the origin of an ISO-compliant driving licence, and confirming data integrity.

Introduction

This part of ISO/IEC 18013 prescribes requirements for the implementation of machine-readable technology on an ISO-compliant driving licence (IDL).

One of the functions of an IDL is to facilitate international interchange. Storing IDL data in machine-readable form supports this function by speeding up data input and eliminating transcription errors. Consequently, the automation and productivity of traffic law enforcement and other traffic safety processes can be improved.

This part of ISO/IEC 18013 allows issuing authorities to customise machine-readable data for domestic use. Apart from international interchange, the use of an IDL as a domestic driving licence thus provides for domestic standardisation and creates a domestic infrastructure capable of processing IDLs issued by other issuing authorities.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 18013-2:2008](https://standards.iteh.ai/catalog/standards/sist/6458f7c4-99d9-4490-9fb1-1b658ec0e8f1/iso-iec-18013-2-2008)

<https://standards.iteh.ai/catalog/standards/sist/6458f7c4-99d9-4490-9fb1-1b658ec0e8f1/iso-iec-18013-2-2008>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 18013-2:2008

<https://standards.iteh.ai/catalog/standards/sist/6458f7c4-99d9-4490-9fb1-1b658ec0e8f1/iso-iec-18013-2-2008>

Information technology — Personal identification — ISO-compliant driving licence

Part 2: Machine-readable technologies

1 Scope

ISO/IEC 18013 establishes guidelines for the design format and data content of an ISO-compliant driving licence (IDL) with regard to human-readable features (ISO/IEC 18013-1), ISO machine-readable technologies (ISO/IEC 18013-2), and access control, authentication and integrity validation (ISO/IEC 18013-3). It creates a common basis for international use and mutual recognition of the IDL without impeding individual countries/states in applying their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs.

The purpose of storing IDL data on machine-readable media on the IDL is to

- increase productivity (of data and IDL use),
- facilitate electronic data exchange, and
- assist in authenticity and integrity validation.

This part of ISO/IEC 18013 thus specifies the following:

- mandatory and optional machine-readable data;
- the logical data structure;
- encoding rules for the machine-readable technologies currently supported.

To prevent unauthorised access to the data contained on a contactless IC (e.g. by eavesdropping), provision is made to protect the privacy of the licence holder via basic access protection [requiring a human-readable and/or machine-readable key/password on the IDL to access the data on the PIC (via protected-channel communication)]. The implementation details of this function however are defined in ISO/IEC 18013-3.

Provision is made for issuing authorities to validate the authenticity and integrity of the mandatory and optional data. In addition, the option of protecting access to optional data (beyond basic access protection) is provided for. The exact mechanism used to achieve such protection (e.g. encryption and/or additional access control) is specified in ISO/IEC 18013-3.

2 Conformance

A driving licence is in conformance with this part of ISO/IEC 18013 if it meets all mandatory requirements specified directly or by reference herein. Compliance with ISO/IEC 18013-1 is not required for compliance with this part of ISO/IEC 18013, except for those parts of ISO/IEC 18013-1 directly referenced in this part of ISO/IEC 18013 outside of Clause 3. Conversely, the incorporation of a machine-readable technology which is

not compliant with this part of ISO/IEC 18013 does not necessarily render the IDL non-compliant with ISO/IEC 18013-1.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 3166-1:2006, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

ISO/IEC 5218:2004, *Information technology — Codes for the representation of human sexes*

ISO/IEC 7812-1:2006, *Identification cards — Identification of issuers — Part 1: Numbering system*

ISO/IEC 7816-5:2004, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers*

ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 8859-1:1998, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

ISO/IEC 18013-1, *Information technology — Personal identification — ISO-compliant driving licence — Part 1: Physical characteristics and basic data set*

ISO/IEC 19785-1:2006, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-3:2007, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19794-2:2005, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

ISO/IEC 19794-4:2005, *Information technology — Biometric data interchange formats — Part 4: Finger image data*

ANSI D20-2003, *Data Element Dictionary For Traffic Records Systems* (April 2003)

IAFIS-IC-0110(V3), *WSQ Gray-scale Fingerprint Image Compression Specification*, Federal Bureau of Investigation, Criminal Justice Information Services Division (1997)

4 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in ISO/IEC 18013-1 and the following apply.

4.1 basic access protection BAP

requiring a human-readable and/or machine-readable key/password on the IDL to access the data on the secure IC via protected-channel communication

4.2 binary coded decimal BCD

binary coding of a sequence of integers using 4 bits for each integer (where the bit weights are 8421) and encoding two integers per byte, and where a 0 digit is appended to the left of an integer sequence containing an uneven number of digits before encoding

NOTE 1 Only unsigned BCD is used in this part of ISO/IEC 18013.

NOTE 2 For purposes of this part of ISO/IEC 18013, the definition of numeric characters in ISO/IEC 18013-1 in terms of ISO/IEC 8859-1 is deemed to be for identification purposes of the numeric characters only, and does not pertain to the manner in which numeric characters have to be encoded. Encoding rules are explicitly specified in this part of ISO/IEC 18013.

EXAMPLE

Integer	BCD
5	0000 0101
20	0010 0000
387	0000 0011 1000 0111

4.3 Biometric Data Block BDB

block of data with a defined format that contains one or more biometric samples or biometric templates

4.4 Biometric Information Record BIR

BioAPI Consortium Patron Format biometric record header

4.5 biometric template

biometric sample (i.e. information obtained from a biometric device, either directly or after further processing) or combination of biometric samples that is suitable for storage as a reference for future comparison

NOTE This definition is an expansion of a definition in ISO/IEC 19785-1.

4.6 card holder

person using an IDL, who is not necessarily the legitimate licence holder

4.7 Common Biometric Exchange File Format CBEFF

file format that promotes interoperability of biometric-based applications and systems by specifying a standard structure for a BIR and a set of abstract data elements and values that can be used to create the header part of a CBEFF-compliant BIR

NOTE This definition is based on descriptive language in ISO/IEC 19785-1.

4.8 compact encoding

encoding method when the memory capacity available for the IDL application does not exceed 5 kB, typically applicable to 2D barcode symbologies, high-coercivity high-density magnetic stripe and limited memory-capacity ICs (PICs and ICs with contacts)

NOTE 1 Compact encoding generates one constructed data object containing all data groups. Selective reading is not possible and the read device reads all data at the same time, whereafter the data is parsed. Using this method for machine-readable technologies with large memory capacity is not recommended as it can result in prolonged reading time.

NOTE 2 Compact encoding may also be used where the total memory capacity exceeds 5 kB (e.g. ICs with contacts and PICs) but where the capacity available to the IDL application is limited due to capacity being reserved for other applications.

4.9

Data Group

DG

collection of related data elements

4.10

dedicated file

DF

4.11

delimiter

D

character used to separate data elements in a machine-readable data stream

4.11.1

data group delimiter

multiplication sign "×" (character D7 of ISO/IEC 8859-1)

4.11.2

field delimiter

division sign "÷" (character F7 of ISO/IEC 8859-1)

4.11.3

sub-field delimiter

sub-delimiter

semicolon ";" (character 3B of ISO/IEC 8859-1)

ISO/IEC 18013-2:2008
<https://standards.iteh.ai/catalog/standards/sist/6458f7c4-99d9-4490-9fb1-1b658ec0e8f1/iso-iec-18013-2-2008>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4.11.4

end of file delimiter

pilcrow "¶" (character B6 of ISO/IEC 8859-1)

4.12

digital signature

data appended to, or cryptographic transformation of, a data string that proves the origin and the integrity of the data string and protects against forgery, e.g. by the recipient of the data string

[ISO/IEC 7816-4]

4.13

elementary file

EF

4.14

integrated circuit

IC

4.15

integrated circuit card

ICC

4.16
logical data structure
LDS

4.17
master file
MF

4.18
proximity integrated circuit
PIC

4.19
proximity integrated circuit card
PICC

4.20
standard encoding
 encoding method when the memory capacity available for the IDL application exceeds 5 kB, typically applicable to ICs (PICs and ICs with contacts) and optical memory

5 Machine-readable functionality of IDLs

The sub-paragraphs that follow specify the functions (mandatory and optional) to be supported by any machine-readable data elements used on an IDL. The optional domestic data elements incorporated at the discretion of an issuing authority may support additional functions than those specified below.

5.1 General principles

The use of machine-readable functionality in IDLs is optional. If used, all the data elements identified in ISO/IEC 18013-1 as mandatory for international interchange, except for the signature and portrait of the licence holder, shall be included in the machine-readable data. The machine-readable data elements may also include any other data / information that appears visually on the IDL (such as the identification of the issuing country), as well as additional data elements not reflected visually on the IDL. No machine-readable data / information shall conflict with the human-readable data / information. Machine-readable data elements shall, except for optional domestic data (see clause 8.8), have the exact same meaning as the human-readable data elements on the IDL.

NOTE A conflict between human-readable data elements and machine-readable data elements may cast suspicion upon the licence holder.

Rewriting, updating, and appending functions may be supported to the extent allowed by the technology (or technologies) used. If implemented, such functions shall comply with the principles set out herein. Security options are established to support authenticity and integrity of machine-readable data.

It shall be possible to read mandatory data without restriction (with the exception of basic access protection in the case of a PIC IDL). Optional data may be protected, in which case the protection mechanism (and associated parameters) shall be noted or referenced. The various protection mechanisms are specified in ISO/IEC 18013-3. The optional domestic data may be protected in any manner without restriction.

Changes to machine-readable data elements by the issuing authority are allowed only to data-elements that do not appear in human-readable format on the IDL. Issuing authorities shall uniquely identify each new version (see clause 8.3) of optional machine-readable data (typically after changing the originally recorded optional data). Issuing authorities shall issue a new IDL when changes to machine-readable data elements will lead to inconsistencies with human-readable data elements on the IDL.

5.2 Mandatory functions

Machine-readable data elements included on an IDL shall support/enable the functions described in the subparagraphs that follow below.

5.2.1 Privilege to drive at time of licensing

Using the IDL to determine (from machine-readable data elements) the driving privileges (and associated restrictions, conditions and validity period(s)) granted to the licence holder by the issuing authority identified on the IDL. It is recognized that this information does not confirm that the issuing authority presently (i.e. at the time when the machine-readable data on an IDL is read by an entity trying to establish a licence holder's driving privileges) considers the licence holder's driving privileges to be valid.

5.2.2 Reference to driving privilege database

Using the machine-readable data elements (such as the licence number) on the IDL to reference records of driving privileges maintained by the issuing authority.

5.2.3 Age verification

Using the machine-readable data elements on the IDL to assure that the licence holder meets various age thresholds for certain products and services, including driving privileges (in the case where the age threshold to drive a particular category of vehicle domestically in the issuing country is lower than the age permitted internationally).

5.3 Optional functions

5.3.1 Identity verification

Using the machine-readable data elements on the IDL to confirm, by way of a visual comparison of the portrait image, that the card holder is the licence holder.

5.3.2 Biographical data verification

Using the machine-readable data elements on the IDL to confirm, by way of visual inspection of the biographical data printed on the portrait side of the card that such data have not been altered.

5.3.3 Evidence of residence

Ability to use the IDL as evidence that the licence holder resided at a specific location at the time the IDL was issued. It is recognized that this information does not confirm that the issuing authority presently considers the licence holder's residential information to be correct.

5.3.4 Biometric authentication

Ability to use a machine-readable biometric template or templates on the IDL to determine whether the card holder is the licence holder by means of a machine-assisted biometric verification process (i.e. a one-to-one match).

5.3.5 Reciprocity of driving privileges

Ability for a country other than the issuing country to use the machine-readable data elements on the IDL to establish whether a mutual recognition agreement (or agreements) exists with the issuing authority.

5.3.6 Document authentication and validation

Ability to reference items on or qualities about the IDL to verify the document is authentic (i.e. produced by the issuing authority reflected both in the human- and machine-readable data) and that no data has been altered since issuing.

6 Machine-readable technologies supported

Technologies suitable for both compact encoding and standard encoding are supported.

For compact encoding, a typical minimum capacity of 300 usable bytes is required.

Given the minimum data capacity needed to support the mandatory data requirements, the IDL may contain any or a combination of the following machine-readable technologies:

- High coercivity high density Magnetic Stripe – Compact encoding, see Annex B.
- Two-dimensional Barcode – Compact encoding, see Annex B.
- IC with contacts – Standard encoding, see Annex C (failing which, compact encoding only if limited memory capacity is available for the IDL application, see Annex B).
- PIC – Standard encoding, see Annex C (failing which, compact encoding only if limited memory capacity is available for the IDL application, see Annex B).
- Optical memory – Standard encoding, see Annex D.

7 Organization of data

Data is organized into eleven data groups, of which each contains data pertaining to a similar function. One data group is mandatory and the others are optional. One data group is reserved for future use.

NOTE Whether or not each group (or individual data element) can be accessed individually depends on the machine-readable technology used.

7.1 Mandatory data

Mandatory data is comprised of the minimum set of data elements required for international interchange (as defined in ISO/IEC 18013-1), with the exception of the signature and portrait.

[ISO/IEC 18013-2:2008](https://standards.iteh.ai/catalog/standards/sist/6458f7c4-99d9-4490-9fb1-1b658ec0e8f1/iso-iec-18013-2-2008)

7.2 Optional data

Optional data is organized into the following groups – licence holder details (DG 2), issuing authority details (DG 3), portrait image (DG 4), signature / usual mark image (DG 5), facial biometric template (DG 6), fingerprint biometric template (DG 7), iris biometric template (DG 8), and domestic data (DG 11). Provision is also made for another as yet undefined biometric template (DG 9), and an additional group reserved for future use (DG 10).

8 Data structure

Details of the data structure will vary depending upon the storage technology(s) used. Conceptually the structure can be visualized as depicted in Figure 1.

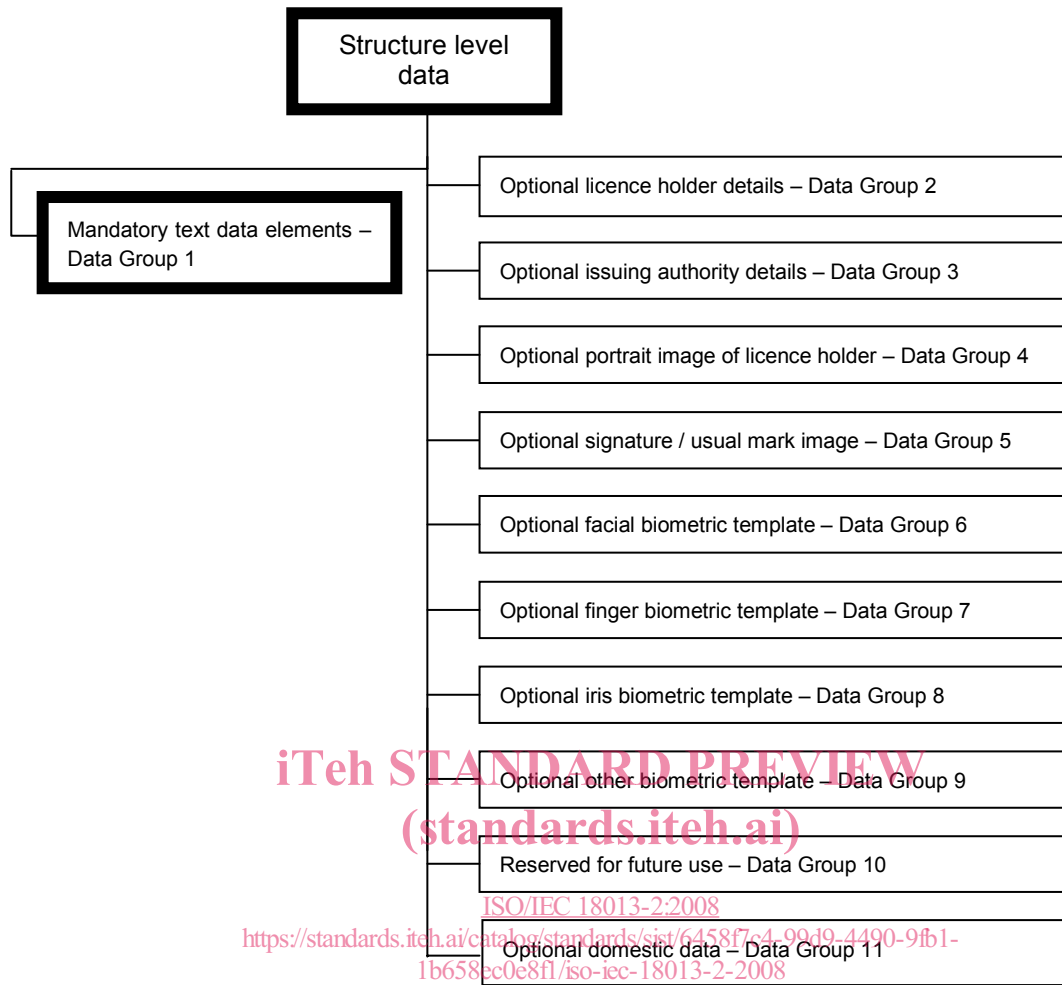


Figure 1 — Conceptual data structure

NOTE This is only a graphical representation. The actual data mapping for each of the machine-readable technologies is specified in the Annexes.

Additional data groups and data elements that are applicable specifically to access control, authentication and integrity validation are specified in ISO/IEC 18013-3.

8.1 Data Group 1: Mandatory text data elements

Data Group 1 consists of nine mandatory elements – demographic data and endorsement/restriction information.

Table 1 — Data Group 1, mandatory text data elements

Name	Fixed or Variable	Field format/length/type	Example
Family name	V	36AS	Smithe-Williams
Given ^a names	V	36AS	Alexander George Thomas
Date of birth (yyyymmdd)	F	8N	19700301
Date of issue (same format as Date of Birth)	F	8N	20020915
Date of expiry (same format as Date of Birth)	F	8N	20070930
Issuing country (per ISO 3166-1)	F	3A	JPN
Issuing authority	V	65ANS	HOKKAIDO PREFECTURAL POLICE ASAHIKAWA AREA PUBLIC SAFETY COMMISSION
Licence number	V	25AN	A290654395164273X
Categories of vehicles/restrictions/conditions (refer to Annex A for field assembly rules)	V	ADNS (also refer to Annex A)	C1;20000315;20100314;93;<=;8000
NOTE	Note the difference between the issuing country code specified in ISO 3166-1, and the issuing country code appearing in Zone 1 of an IDL as specified in Appendix F of ISO/IEC 18013-1.		
^a	No titles and/or suffixes shall be included.		

The assembly of the categories of vehicles/restrictions/conditions field is defined in Annex A. Encoding specifics vary slightly depending upon the technology mapping employed and is defined in Annexes B, C and D in accordance with the machine-readable medium included on the card. The following general format (repeated as necessary) is adhered to:

[category] ; [issue date] ; [expiry date] ; [restriction/condition code] ; [restriction/condition sign] ; [restriction/condition value]

NOTE Spaces (periods) have been inserted before and after the sub-field delimiter above for ease of reading only.

8.2 Data Group 2: Optional licence holder details

Data Group 2 consists of seven optional data elements that provide supplemental descriptive information. Any or all data elements may be present for a particular implementation.