

PUBLIC

PERSONAL DATA PROTECTION POLICY

AUTHOR(S) : V. Dumond B. Andreasson
DOCUMENT NUMBER : WLM-TSP-F224
VERSION : 2.0
STATUS : Final
SOURCE : Worldline
DATE OF THE DOCUMENT : 27/04/2020
NUMBER OF PAGES : 14

OWNER : Comité MediaCert

Table of contents

Table of contents	2
List of changes	3
1 Introduction	4
2 Definitions.....	5
3 Purpose and Legal Basis for Processing	6
3.1 Purpose	6
3.2 Legal Basis for the Processing	6
4 Categories of Personal Data.....	7
5 Data Protection Officer.....	8
6 Sub-Contractors and Transfers of Personal Data to Third Countries, and Recipients of Personal Data	9
7 Data Retention.....	10
8 Method of Collection and Processing of Your Personal Data	11
9. Your Rights as a Data Subject.....	12
9.1 Right of Access to Personal Data	12
9.2 Right to Rectification of Personal Data	12
9.3 Right to Erasure of Personal Data	12
9.4 Right to Restrict Processing	12
9.5 Right to Object Processing.....	13
9.6 Right to Withdraw your Consent.....	13
9.7 Right to Data Portability	13
9.8 Right to Lodge a Complaint with a Data Protection Authority	13
10 End of Document	14

List of changes

Version	Date	Description	Author(s)
1.0	11/03/2019	Creation of document	B. Andreasson V. Dumond F. Da Silva
2.0	27/04/2020	Revision 2020 of the document	V. Dumond B. Andreasson

1 Introduction

The purpose of this document is to explain to you why and how the *Trust Service Provider* MediaCert (hereafter referred to as "TSP MediaCert"), through its OTU¹ Registration and Certification Authorities, is processing your personal data to enable you to make an electronic signature based on an electronic Certificate.

¹ OTU = One Time Usage

2 Definitions

Trust Service Provider MediaCert

As part of its activities, Worldline has set up an infrastructure dedicated to trust services or Trust Service Provider called "MediaCert". The different trust services offered by the **Trust Service Provider MediaCert** include the OTU electronic signature service, which relies on two Authorities, one for Registration and the other for Certification. The implemented OTU electronic signature service requires the issuance of an Electronic Certificate on behalf of the natural person wishing to make a signature. It therefore requires a certain number of processing of personal data.

This Policy applies to processing that is carried out by the MediaCert OTU Registration and Certification Authority as part of this electronic signature service.

Registration Authority

The Registration Authority (RA) referred to in this document is the entity to which your Organization sends requests for the creation of Electronic Certificates on your behalf, and identifies and authenticates you with the help of the Organization.

Certification Authority

The Certifying Authority designated in this document is the entity that will produce the Certificates at the request of the Registration Authority.

Authentication

This refers to an electronic process that confirms your identification.

Certificate

This designates an electronic certificate with a limited lifespan (a few minutes), produced dynamically by the Certification Authority at the request of the Organization during the electronic signature process. With the lifespan of the mentioned certificate being very short, it can be used in one unique signature session only. This is referred to as "certificate for unique usage" or "OTU certificate" (One Time Usage) or also "instant certificate".

This certificate identifies you.

Certificate Request

Request formulated for you upon your request by the Organization for you to obtain an Electronic Certificate so that you can sign.

Identification

A process that establishes your identity.

Organization

In this document it refers to the entity that allows you to sign dematerialized documents.

3 Purpose and Legal Basis for Processing

3.1 Purpose

To be able to apply an electronic signature based on a Certificate, your identification is necessary.

The purpose of the processing being carried out is therefore for the concerned Registration Authority and Certification Authority for the issuing of your Certificate to:

- Constitute your identification and allow your authentication, to generate a Certificate on your behalf.

Be able to process and store the activation data that will trigger your signature under your control.
- Support the identification of your identity in the Certificate by providing necessary evidence, if required, by keeping the items in the registration file.
- Meet the obligations imposed on the certification providers in the context of the audits they have to pass, to justify compliance with the chosen certification level, the identification functions assigned to the electronic signature, the state of the art, and applicable standards.

The requirements expressed here above explain:

- The processing of your personal data described below, by the Registration Authority in the context of requests for the creation of Certificates issued on your behalf.
- The transfer of the same data by the Registration Authority to the Certification Authority so that it can produce the Certificates and allow you to sign.
- And respectively for both functions to fulfill their obligations as trusted actors.

3.2 Legal Basis for the Processing

The legal basis of the processing for the Registration Authority and Certification Authority concerned by the issuing of your Certificate is based on your consent:

- According to Article 6 1.a) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

4 Categories of Personal Data

The personal data collected and transmitted by the Organization to the Registration Authority are:

- As a minimum the following data:
 - Your first name and your surname.
 - Your date and place of birth.
 - A copy of your valid identity document including your photo.
- Depending on the case and the applied signature cycle, also:
 - Your title.
 - Your mailing address.
 - Your phone number.
 - Your email address.
 - Or any other legally recognized element to support your identity.

We also keep information and traces in our trust infrastructure that may contain personal data, such as:

- Those appearing in the registration information.
- Those included in the Certificate generation requests.
- Those appearing in possible requests for revocation of a Certificate.
- Those appearing in the Certificates.
- In addition, we keep the personal data attached to your consents provided in connection with our provision of trust services.

In addition, specific checks may possibly be carried out at the request of the Organization to submit your ID documents to an automated control, which may, under legally prescribed conditions, be completed by a human analysis to check the consistency of the fields. The Organization may give us access, in this hypothesis, to the results of these controls.

If these controls were to be carried out directly by us on our initiative to respond to regulatory requirements, they will be communicated to you in detail by the Organization with their deployment methods and will be subject to your explicit consent.

5 Data Protection Officer

The contact details for the Data Protection Officer for TSP MediaCert, for questions regarding personal data protection, are:

DPO Worldline
23 rue de la Pointe
Zone Industrielle A
59113 SECLIN France
dpo-worldline-france@worldline.com

6 Sub-Contractors and Transfers of Personal Data to Third Countries, and Recipients of Personal Data

Your personal data may be communicated to our subcontractors to TSP MediaCert for the sole purpose of performing the processing for which they were collected. In this context, the service providers are subcontractors of personal data in the sense of the regulation, they act on the instructions and on behalf of TSP MediaCert, and they are required to comply with the rules for the TSP MediaCert trust services. They are not allowed to sell or disclose your personal data to other third parties.

The recipients of your personal data are:

- In addition to the concerned RA and CA.
- The provider responsible for carrying out a consistency check of the documents justifying your identity, if this processing is requested by the RA on its initiative.

There is no transfer of personal data outside the European Union.

7 Data Retention

All of the aforementioned information is kept for eight (8) years by the Registration Authority in the registration file in electronic format associated with the issuance of the Certificate.

The personal data kept by TSP MediaCert do not leave the European Union and are stored securely by TSP MediaCert.

8 Method of Collection and Processing of Your Personal Data

The Registration Authority relies on the Organization, which has proposed you to sign a document, to collect the pieces of information allowing your identification, in order to be able to provide you, via the Certification Authority, with a Certificate in your name.

9. Your Rights as a Data Subject

Your rights in accordance with the applicable laws and regulations (GDPR) are resumed here below:

9.1 Right of Access to Personal Data

You have the right to request access to your personal data.

- I. The right of access may be exercised in writing:
 - Either through the Organization which will inform us of your request and verify it.
 - Or by mail to the contact address to TSP MediaCert, accompanied by a copy of an ID document, preferably by registered mail with acknowledgment of receipt.

Comité MediaCert
Worldline
23 rue de la Pointe
Zone Industrielle A
59113 SECLIN France

- II. You can also make requests concerning your personal data via the following e-mail address: dl-mediacert-tsp@worldline.com

9.2 Right to Rectification of Personal Data

You can request the correction of your personal data. It is however specified that the personal data used for your identification and your authentication, which were communicated to us by the Organization with your agreement during the process of electronic signature or of the constitution of the registration file, remain in the historical trace of the transaction and the operated electronic signature, until the exhaustion of the purpose for which these personal data were collected and the processing operations carried out in such a way as to ensure the legal security and legality of the performed operation.

9.3 Right to Erasure of Personal Data

You can request the deletion of your personal data. It is however specified that the personal data used for your identification and your authentication, which were communicated to us by the Organization with your agreement during the process of electronic signature or of the constitution of the registration file, remain in the historical trace of the transaction and the operated electronic signature, until the exhaustion of the purpose for which these personal data were collected and the processing operations carried out in such a way as to ensure the legal security and legality of the performed operation. Once the purpose is exhausted, your data will be destroyed and their destruction will be documented.

9.4 Right to Restrict Processing

You have the right to obtain a restriction of the processing when one of the following cases applies:

- a) You dispute the accuracy of the personal data for a period of time allowing the controller to verify the accuracy of the personal data.
- b) The processing is unlawful and the data subject objects to the erasure and instead requires the restriction of their use.
- c) The controller no longer needs personal data for processing purposes, but it is still necessary for the data subject to ascertain, exercise or defend rights in court.
- d) You object to the processing under Article 21 (1) of the GDPR during the verification as to whether the legitimate grounds pursued by the data controller take precedence over those of the data subject.

9.5 Right to Object Processing

It is imperative that your electronic signature is based on verified identity elements. Consequently, if you make the choice to sign electronically, you must accept that the Organization that offers you the electronic signature can transfer the personal data that make it possible to achieve this purpose of identification to the Certification Authority, so that it can thus meet its obligations as trusted third party.

This being the case, you have the right to oppose the processing of your data by TSP MediaCert by Worldline.

In this hypothesis, it will be necessary to see what alternative modes that are proposed to you by the Organization to be able to sign.

9.6 Right to Withdraw your Consent

It is as easy to withdraw as to give consent. You are informed before giving your consent. If you agree to consent to the processing of your data, it is to allow the Registration Authority to process these so that the Certification Authority can issue a certificate that allows you to electronically sign a document. In this context, withdrawal of consent cannot compromise the lawfulness of consent-based processing prior to withdrawal.

9.7 Right to Data Portability

You have the right to portability of data in the same format as communicated to us by the Organization.

9.8 Right to Lodge a Complaint with a Data Protection Authority

You have the right to lodge a complaint with the data protection authority CNIL:

3 Place de Fontenoy
TSA 80715
75334 PARIS CEDEX, France

10 End of Document