

[MS-P3P]:

Internet Explorer Platform for Privacy Preferences (P3P) Standards Support Document

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: <http://www.microsoft.com/interop/osp>) or the Community Promise (available here: <http://www.microsoft.com/interop/cp/default.mspx>). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplq@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
03/17/2010	0.1	New	Released new document.
03/26/2010	1.0	None	Introduced no new technical or language changes.
05/26/2010	1.2	None	Introduced no new technical or language changes.
09/08/2010	1.3	Major	Significantly changed the technical content.
10/13/2010	1.4	Minor	Clarified the meaning of the technical content.
02/10/2011	2.0	No change	Introduced no new technical or language changes.

Table of Contents

1	Introduction	5
1.1	Glossary	5
1.2	References.....	5
1.2.1	Normative References	5
1.2.2	Informative References	5
1.3	Microsoft Implementations.....	5
1.4	Standards Support Requirements	6
1.5	Notation	6
2	Standards Support Statements.....	8
2.1	Normative Variations.....	8
2.1.1	[W3C-P3P1.0] Section 2.3.2.1.2, Wildcards in policy reference files	8
2.1.2	[W3C-P3P1.0] Section 2.3.2.2, The META and POLICY-REFERENCES elements	8
2.1.3	[W3C-P3P1.0] Section 2.3.2.3.4, Error handling for policy reference file and policy lifetimes.....	9
2.1.4	[W3C-P3P1.0] Section 2.3.2.5, The INCLUDE and EXCLUDE elements.....	9
2.1.5	[W3C-P3P1.0] Section 2.3.2.6, The HINT element	9
2.1.6	[W3C-P3P1.0] Section 2.3.2.7, The COOKIE-INCLUDE and COOKIE-EXCLUDE elements	10
2.1.7	[W3C-P3P1.0] Section 2.3.4, Forms and Related Mechanisms	10
2.1.8	[W3C-P3P1.0] Section 2.4.1, Non-ambiguity.....	11
2.1.9	[W3C-P3P1.0] Section 3.2.1, The POLICIES element	11
2.1.10	[W3C-P3P1.0] Section 3.2.4, The ENTITY element	11
2.1.11	[W3C-P3P1.0] Section 3.2.5, The ACCESS element.....	12
2.1.12	[W3C-P3P1.0] Section 3.2.6, The DISPUTES element.....	12
2.1.13	[W3C-P3P1.0] Section 3.2.7, The REMEDIES element	14
2.1.14	[W3C-P3P1.0] Section 3.3.2, The CONSEQUENCE element	14
2.1.15	[W3C-P3P1.0] Section 3.3.3, The NON-IDENTIFIABLE element.....	14
2.1.16	[W3C-P3P1.0] Section 3.3.4, The PURPOSE element.....	15
2.1.17	[W3C-P3P1.0] Section 3.3.5, The RECIPIENT element.....	15
2.1.18	[W3C-P3P1.0] Section 3.3.6, The RETENTION element.....	16
2.1.19	[W3C-P3P1.0] Section 3.3.7, The DATA-GROUP and DATA elements	17
2.1.20	[W3C-P3P1.0] Section 3.4, Categories and the CATEGORIES element	18
2.1.21	[W3C-P3P1.0] Section 3.5, Extension Mechanism: the EXTENSION element.....	18
2.1.22	[W3C-P3P1.0] Section 4, Compact Policies	19
2.1.23	[W3C-P3P1.0] Section 5.5, Basic Data Structures	19
2.1.24	[W3C-P3P1.0] Section 5.6.1, User Data.....	19
2.1.25	[W3C-P3P1.0] Section 5.6.2, Third Party Data	20
2.2	Clarifications	20
2.2.1	[W3C-P3P1.0] Section 2.2, Locating Policy Reference Files	20
2.2.2	[W3C-P3P1.0] Section 2.3.2.1.2, Wildcards in policy reference files	20
2.2.3	[W3C-P3P1.0] Section 2.3.2.3.3, Requesting Policies and Policy Reference Files.....	21
2.2.4	[W3C-P3P1.0] Section 2.3.4, Forms and Related Mechanisms	21
2.2.5	[W3C-P3P1.0] Section 2.4.1, Non-ambiguity.....	21
2.2.6	[W3C-P3P1.0] Section 2.4.2, Multiple Languages	22
2.2.7	[W3C-P3P1.0] Section 2.4.8, Asynchronous Evaluation	22
2.2.8	[W3C-P3P1.0] Section 3.2.2, The POLICY element.....	22
2.2.9	[W3C-P3P1.0] Section 3.6, User Preferences	23
2.2.10	[W3C-P3P1.0] Section 4.1, Referencing compact policies.....	23
2.2.11	[W3C-P3P1.0] Section 5.3, The DATA-DEF and DATA-STRUCT elements.....	25

2.3 Error Handling	26
2.4 Security.....	26
3 Change Tracking.....	27
4 Index	28

1 Introduction

This document describes the level of support provided by Windows® Internet Explorer® 7, Windows® Internet Explorer® 8, and Windows® Internet Explorer® 9 for *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification* [W3C-P3P1.0] W3C Recommendation 16 April 2002. Internet Explorer displays webpages written in HTML.

The [W3C-P3P1.0] specification may contain guidance for authors of webpages and browser users, in addition to user agents (browser applications). Statements found in this document apply only to normative requirements in the specification targeted to user agents, not those targeted to authors.

1.1 Glossary

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, <http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624>, as an additional source.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>

[W3C-P3P1.0] Cranor, L., Langheinrich M., Marchiori, M., Presler-Marshall, M., and Reagle, J., "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification", W3C Recommendation 16 April 2002, <http://www.w3.org/TR/P3P/>

1.2.2 Informative References

None.

1.3 Microsoft Implementations

The following Microsoft products implement some portion of the [W3C-P3P1.0] specification:

- Windows® Internet Explorer® 7
- Windows® Internet Explorer® 8
- Windows® Internet Explorer® 9

In addition, each version of Windows® Internet Explorer® implements multiple document modes, which can vary individually in their support of the standard. The following table lists the document modes available in each version of Internet Explorer.

Browser version	Document modes supported
Internet Explorer 7	Quirks mode

Browser version	Document modes supported
	Standards mode
Internet Explorer 8	Quirks mode IE7 mode IE8 mode
Internet Explorer 9	Quirks mode IE7 mode IE8 mode IE9 mode

Throughout this document, the document mode appears first followed by the browser version in parentheses. Only those document modes and versions of Internet Explorer for which there is a variation note will be listed. If the document mode is not listed, conformance to the specification can be assumed.

Note "Standards mode" in Internet Explorer 7 and "IE7 mode" in Internet Explorer 8 refer to the same document mode. "IE7 mode" is the preferred way of referring to this document mode across all versions of the browser. In addition, "IE5 mode" and "Quirks mode" refer to the same document mode in Internet Explorer 9.

1.4 Standards Support Requirements

To conform to [\[W3C-P3P1.0\]](#), a user agent must implement all required portions of the specification. Any optional portions that have been implemented must also be implemented as described by the specification. Normative language is usually used to define both required and optional portions. (For more information, see [\[RFC2119\]](#).)

The following table lists the sections of [\[W3C-P3P1.0\]](#) and whether they are considered normative or informative.

Sections	Normative/Informative
1-3	Informative
4-18	Normative
19-23	Informative
24	Normative
Appendices A-B	Informative

1.5 Notation

The following notations are used in this document to differentiate between notes of clarification, variation from the specification, and extension points.

Notation	Explanation
C####	This identifies a clarification of ambiguity in the target specification. This includes imprecise statements, omitted information, discrepancies, and errata. This does not include data formatting clarifications.

Notation	Explanation
V####	This identifies an intended point of variability in the target specification such as the use of MAY, SHOULD, or RECOMMENDED. (See RFC2119 .) This does not include extensibility points.
E####	Because the use of extensibility points (such as optional implementation-specific data) can impair interoperability, this profile identifies such points in the target specification.

2 Standards Support Statements

This section contains a full list of variations, clarifications, and extension points in the Microsoft implementation of [\[W3C-P3P1.0\]](#).

- Section [2.1](#) includes only those variations that violate a MUST requirement in the target specification.
- Section [2.2](#) describes further variations from MAY and SHOULD requirements.
- Section [2.3](#) identifies variations in error handling.
- Section [2.4](#) identifies variations that impact security.

2.1 Normative Variations

The following sections detail the normative variations from MUST requirements in [\[W3C-P3P1.0\]](#).

2.1.1 [W3C-P3P1.0] Section 2.3.2.1.2, Wildcards in policy reference files

V0001:

The specification states:

URIs represented in policy reference files MUST be properly escaped, as described in [URI], except:

Literal '*'s in URIs MUST be escaped in policy reference files (i.e., they MUST be represented as "%2A"). Any '*' present in a URI within a policy reference file will be taken as representing the asterisk wildcard character. Consequently, P3P user agents MUST properly un-escape a URI given in a policy reference file, according to [URI], before trying to match it against an internally represented URI, but only after recognizing any literal '*' present as the asterisk wildcard character.

All Document Modes (All Versions)

The %2A character reference is not unescaped before matching. For example, "/p3ptest/%2A*" will not match "/p3ptest/**".

2.1.2 [W3C-P3P1.0] Section 2.3.2.2, The META and POLICY-REFERENCES elements

V0002:

The specification states:

<META>
The META element contains a complete policy reference file. Optionally, one POLICIES element can follow. META can also contain one or more one or more EXTENSION elements (cf. section 3.5), as well as an xml:lang attribute (see section 2.4.2), to indicate the language in which its content is expressed.

All Document Modes (All Versions)

The **policies** element, **extension** element, and **xml:lang** attribute are not supported.

V0003:

The specification states:

```
<POLICY-REFERENCES>
This element MAY contain one or more POLICY-REF (policy reference) elements. It MAY
also contain one EXPIRY element (indicating their expiration time), one or more
HINT element, and one or more EXTENSION element (cf. section 3.5).
```

All Document Modes (All Versions)

The **hint** and **extension** elements are not supported.

2.1.3 [W3C-P3P1.0] Section 2.3.2.3.4, Error handling for policy reference file and policy lifetimes

V0004:

The specification states:

```
The following situations have their semantics specifically defined:

1.An absolute expiry date in the past renders the policy reference file (or
policies) useless, as does an invalid or malformed expiry date, whether relative or
absolute. In this case, user agents MUST act as if NO policy reference file (or
policies) is available. See section 2.4.7 "Absence of Policy Reference File" for
the required procedure in such cases.
2.A relative expiration time shorter than 86400 seconds (1 day) is considered to be
equal to 86400 seconds.
3.When a policy reference file contains more than one EXPIRY element, the first one
takes precedence for determining the lifetime of the policy reference file.
```

All Document Modes (All Versions)

Malformed relative expiration dates in policy reference files are treated as valid.

2.1.4 [W3C-P3P1.0] Section 2.3.2.5, The INCLUDE and EXCLUDE elements

V0005:

The specification states:

```
It is legal, but pointless, to supply an EXCLUDE element without any INCLUDE
elements; in that case, the EXCLUDE element MUST be ignored by user agents.
```

All Document Modes (All Versions)

The **METHOD** element is not supported for the **INCLUDE** and **EXCLUDE** elements.

2.1.5 [W3C-P3P1.0] Section 2.3.2.6, The HINT element

V0006:

The specification states:

A site may declare a policy reference for itself using the well-known location, the P3P response header, or the HTML/XHTML link tag. It MAY further provide a hint to additional policy references, such as those declared by other sites.

All Document Modes (All Versions)

The **HINT** element is not supported.

2.1.6 [W3C-P3P1.0] Section 2.3.2.7, The **COOKIE-INCLUDE** and **COOKIE-EXCLUDE** elements

V0007:

The specification states:

The policy that applies to a cookie applies until the policy expires, even if the associated policy reference file expires prior to policy expiry (but after the cookie was set). If the policy associated with a cookie has expired, then the user agent SHOULD reevaluate the cookie policy before sending the cookie. In addition, user agents MUST use only non-expired policies and policy reference files when evaluating new set-cookie events.

All Document Modes (All Versions)

The **COOKIE-INCLUDE** and **COOKIE-EXCLUDE** elements are not supported.

2.1.7 [W3C-P3P1.0] Section 2.3.4, Forms and Related Mechanisms

V0008:

The specification states:

...user agents SHOULD check the well-known location on the host of the action URI to attempt to find a policy reference file that covers the action URI. If this does not provide a P3P policy to cover the action URI, then a user agent MAY try to retrieve the policy reference file by using the HINT mechanism on the action URI, and/or by issuing a HEAD request to the action URI before actually submitting any data in order to find the policy in effect.

All Document Modes (All Versions)

Policies are downloaded only when the user requests to see the policy for a particular URI. To see policies, click the **Tools** menu, click **Internet Options**, and then click the **Privacy** tab.

V0009:

The specification states:

In case the underlying application does not understand the HEAD request and no policy has been predeclared for the action URI in question, user agents MUST assume that no policy is in effect and SHOULD inform the user about this or take the

corresponding actions according to the user's preferences.

All Document Modes (All Versions)

Action URIs are not checked. Users are not informed that action URIs have no policy nor that a full P3P policy is missing.

V0010:

The specification states:

User agents MUST assume that all data elements are collected under every circumstance.

All Document Modes (All Versions)

Action URIs are not checked. Collecting data elements is not performed.

2.1.8 [W3C-P3P1.0] Section 2.4.1, Non-ambiguity

V0011:

The specification states:

If an HTML (resp. XHTML) file includes HTML (resp. XHTML) link tag references to more than one policy reference file, P3P user agents MUST ignore all references after the first one.

All Document Modes (All Versions)

When more than one policy reference file is included, the last policy reference file is used.

2.1.9 [W3C-P3P1.0] Section 3.2.1, The POLICIES element

V0012:

The specification states:

```
policies = `<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1" ` [xml-lang] `>`  
[expiry]  
[dataschema]  
*policy  
"</POLICIES>"
```

All Document Modes (All Versions)

When multiple policies are specified, all their statements are merged into a single policy that is then presented to the user.

2.1.10 [W3C-P3P1.0] Section 3.2.4, The ENTITY element

V0013:

The specification states:

```
entity = "<ENTITY>"
*extension
entitydescription
*extension
"</ENTITY>"

entitydescription = "<DATA-GROUP>"
`<DATA ref="#business.name"/>` PCDATA "</DATA>"
*(`<DATA ref="#business.` string `"/>` PCDATA "</DATA>")
"</DATA-GROUP>"
```

All Document Modes (All Versions)

The **ENTITY** element is not required to contain any **DATA-GROUP** elements.

2.1.11 [W3C-P3P1.0] Section 3.2.5, The ACCESS element

V0014:

The specification states:

```
access = "<ACCESS>"
*extension
access_disclosure
*extension
"</ACCESS>"

access_disclosure = "<nonident/>" | ; Identified Data is Not Used
"<all/>" | ; All Identifiable Information
"<contact-and-other/>" | ; Identified Contact Information and
                        Other Identified Data
"<ident-contact/>" | ; Identifiable Contact Information
"<other-ident/>" | ; Other Identified Data
"<none/>" ; None
```

All Document Modes (All Versions)

Subelements are not validated. All **ACCESS** elements and subelements are displayed, including cases when no subelements are present.

2.1.12 [W3C-P3P1.0] Section 3.2.6, The DISPUTES element

V0015:

The specification states:

```
<DISPUTES>
Describes dispute resolution procedures that may be followed for disputes about a
services' privacy practices, or in case of protocol violation.

resolution-type (mandatory attribute)
takes one of the following four values:

Customer Service [service]
```

Individual may complain to the Web site's customer service representative for resolution of disputes regarding the use of collected data. The description **MUST** include information about how to contact customer service.

Independent Organization [independent]

Individual may complain to an independent organization for resolution of disputes regarding the use of collected data. The description **MUST** include information about how to contact the third party organization.

Court [court]

Individual may file a legal complaint against the Web site.

Applicable Law [law]

Disputes arising in connection with the privacy statement will be resolved in accordance with the law referenced in the description.

service (mandatory attribute)

URI of the customer service Web page or independent organization, or URI for information about the relevant court or applicable law

verification

URI or certificate that can be used for verification purposes. It is anticipated that seal providers will provide a mechanism for verifying a site's claim that they have a seal.

short-description

A short human readable description of the name of the appropriate legal forum, applicable law, or third party organization; or contact information for customer service if not already provided at the service URI. No more than 255 characters.

All Document Modes (All Versions)

The following variations apply:

- The **service** and **resolution-type** attributes are not mandatory.
- The **verification** attribute is not supported.
- The **service** and **short-description** attributes are supported only in conjunction with the **service** and **independent** resolution-type values.

V0016:

The specification states:

The DISPUTES element can contain a LONG-DESCRIPTION element, where a human readable description is present: this should contain the name of the appropriate legal forum, applicable law, or third party organization; or contact information for customer service if not already provided at the service URI.

<LONG-DESCRIPTION>

This element contains a (possibly long) human readable description.

All Document Modes (All Versions)

The **LONG-DESCRIPTION** element is not supported.

2.1.13 [W3C-P3P1.0] Section 3.2.7, The REMEDIES element

V0017:

The specification states:

Each DISPUTES element SHOULD contain a REMEDIES element that specifies the possible remedies in case a policy breach occurs.

<REMEDIES>

Remedies in case a policy breach occurs.

The REMEDIES element must contain one or more of the following:

<correct/>

Errors or wrongful actions arising in connection with the privacy policy will be remedied by the service.

<money/>

If the service provider violates its privacy policy it will pay the individual an amount specified in the human readable privacy policy or the amount of damages.

<law/>

Remedies for breaches of the policy statement will be determined based on the law referenced in the human readable description.

All Document Modes (All Versions)

The **REMEDIES** element is not supported.

2.1.14 [W3C-P3P1.0] Section 3.3.2, The CONSEQUENCE element

V0018:

The specification states:

<CONSEQUENCE>

Consequences that can be shown to a human user to explain why the suggested practice may be valuable in a particular instance even if the user would not normally allow the practice.

consequence = "<CONSEQUENCE>"

PCDATA

"</CONSEQUENCE>"

All Document Modes (All Versions)

The **CONSEQUENCE** element is not supported.

2.1.15 [W3C-P3P1.0] Section 3.3.3, The NON-IDENTIFIABLE element

V0019:

The specification states:

If the NON-IDENTIFIABLE element is present in any STATEMENT elements in a policy, then a human readable explanation of how the data is anonymized MUST be included or linked to at the discURI.

All Document Modes (All Versions)

The **NON-IDENTIFIABLE** element is not supported.

2.1.16 [W3C-P3P1.0] Section 3.3.4, The PURPOSE element

V0020:

The specification states:

Each STATEMENT element that does not include a NON-IDENTIFIABLE element MUST contain a PURPOSE element that contains one or more purposes of data collection or uses of data.

All Document Modes (All Versions)

If the **NON-IDENTIFIABLE** element is missing, **STATEMENT** elements are not required to contain **PURPOSE** elements.

V0021:

The specification states:

<PURPOSE>
purposes for data processing relevant to the Web.
The PURPOSE element MUST contain one or more sub-elements.

All Document Modes (All Versions)

The **PURPOSE** element is not required to contain any subelements.

V0022:

The specification states:

Each type of purpose (with the exception of current) can have the following optional attribute:

Required
Whether the purpose is a required practice for the site.

All Document Modes (All Versions)

The **required** attribute is not supported. No additional information is displayed when the **required** attribute is specified.

2.1.17 [W3C-P3P1.0] Section 3.3.5, The RECIPIENT element

V0023:

The specification states:

Each STATEMENT element that does not include a NON-IDENTIFIABLE element MUST contain a RECIPIENT element that contains one or more recipients of the collected

data. Sites **MUST** classify their recipients into one or more of the six recipients specified.

<RECIPIENT>

the legal entity, or domain, beyond the service provider and its agents where data may be distributed.

The RECIPIENT element **MUST** contain one or more sub-elements.

All Document Modes (All Versions)

The **recipient** element is not required to contain any subelements.

V0024:

The specification states:

Each of the above tags can optionally contain:

- one or more recipient-description tags, containing a description of the recipient;
- with the exception of <ours>, a required attribute: this attribute is defined exactly as the analogous attribute in the PURPOSE tag, indicating whether opt-in/opt-out of sharing is available (and, its default value is always).

All Document Modes (All Versions)

The **required** attribute is not supported when specified on children of the **PURPOSE** element.

2.1.18 [W3C-P3P1.0] Section 3.3.6, The RETENTION element

V0025:

The specification states:

Each STATEMENT element that does not include a NON-IDENTIFIABLE element **MUST** contain a RETENTION element that indicates the kind of retention policy that applies to the data referenced in that statement.

All Document Modes (All Versions)

STATEMENT elements that do not contain a **NON-IDENTIFIABLE** child element are not required to contain a **RETENTION** element containing at least one subchild.

V0026:

The specification states:

<RETENTION>

the type of retention policy in effect

The RETENTION element **MUST** contain one of the following:

<no-retention/>

Information is not retained for more than a brief period of time necessary to make use of it during the course of a single online interaction. Information **MUST** be destroyed following this interaction and **MUST NOT** be logged, archived, or otherwise

stored. This type of retention policy would apply, for example, to services that keep no Web server logs, set cookies only for use during a single session, or collect information to perform a search but do not keep logs of searches performed.

<stated-purpose/>

For the stated purpose: Information is retained to meet the stated purpose. This requires information to be discarded at the earliest time possible. Sites **MUST** have a retention policy that establishes a destruction time table. The retention policy **MUST** be included in or linked from the site's human-readable privacy policy.

<legal-requirement/>

As required by law or liability under applicable law: Information is retained to meet a stated purpose, but the retention period is longer because of a legal requirement or liability. For example, a law may allow consumers to dispute transactions for a certain time period; therefore a business may for liability reasons decide to maintain records of transactions, or a law may affirmatively require a certain business to maintain records for auditing or other soundness purposes. Sites **MUST** have a retention policy that establishes a destruction time table. The retention policy **MUST** be included in or linked from the site's human-readable privacy policy.

<business-practices/>

Determined by service provider's business practice: Information is retained under a service provider's stated business practices. Sites **MUST** have a retention policy that establishes a destruction time table. The retention policy **MUST** be included in or linked from the site's human-readable privacy policy.

<indefinitely/>

Indefinitely: Information is retained for an indeterminate period of time. The absence of a retention policy would be reflected under this option. Where the recipient is a public fora, this is the appropriate retention policy.

All Document Modes (All Versions)

The **RETENTION** element is not required to contain any subelements.

2.1.19 [W3C-P3P1.0] Section 3.3.7, The DATA-GROUP and DATA elements

V0027:

The specification states:

<DATA-GROUP>

describes the data to be transferred or inferred
base

base URI ([URI]) for URI references present in ref attributes. When this attribute is omitted, the default value is the URI of the P3P base data schema (<http://www.w3.org/TR/P3P/base>). When the attribute appears as an empty string (""), the base is the local document.

<DATA>

describes the data to be transferred or inferred
ref (mandatory attribute)

URI reference ([URI]), where the fragment identifier part denotes the name of a data element/set, and the URI part denotes the corresponding data schema. In case the URI part is not present, if the DATA element is contained within a DATA-GROUP element, then the default base URI is assumed to be the URI of the base attribute. In the other cases, as usual, the default base URI is a same-document reference

([URI]).

Remember that names of data elements and sets are case-sensitive (so, for example, user.gender is different from USER.GENDER or User.Gender).

optional

indicates whether or not the site requires visitors to submit this data element to access a resource or complete a transaction; "no" indicates that the data element is not optional (it is required), while "yes" indicates that the data element is optional. The default is "no." The optional attribute is used only in policies (not in data schema definitions).

All Document Modes (All Versions)

The following variations apply:

- Only the explanatory text for each **DATA-GROUP** element that is present in a **DATA** element is displayed.
- The **ref** and **base** attributes of the **DATA-GROUP** element are not supported. The data types are not validated against the base URI.

2.1.20 [W3C-P3P1.0] Section 3.4, Categories and the CATEGORIES element

V0028:

The specification states:

```
categories = "<CATEGORIES>" 1*category "</CATEGORIES>"

category = "<physical/>"      | ; Physical Contact Information
"<online/>"                  | ; Online Contact Information
"<uniqueid/>"                | ; Unique Identifiers
"<purchase/>"                | ; Purchase Information
"<financial/>"                | ; Financial Information
"<computer/>"                | ; Computer Information
"<navigation/>"              | ; Navigation and Click-stream Data
"<interactive/>"             | ; Interactive Data
"<demographic/>"             | ; Demographic and Socioeconomic Data
"<content/>"                  | ; Content
"<state/>"                    | ; State Management Mechanisms
"<political/>"                | ; Political Information
"<health/>"                   | ; Health Information
"<preference/>"               | ; Preference Data
"<location/>"                 | ; Location Data
"<government/>"              | ; Government-issued Identifiers
"<other-category>"           PCDATA "</other-category>" ; Other
```

All Document Modes (All Versions)

The **CATEGORIES** element is not required to contain any subelements. Empty **CATEGORIES** elements are ignored.

2.1.21 [W3C-P3P1.0] Section 3.5, Extension Mechanism: the EXTENSION element

V0029:

The specification states:

```
extension = "<EXTENSION" [" optional=" `"` ("yes"|"no") `"] ">" PCDATA "</EXTENSION>"
```

All Document Modes (All Versions)

The **extension** element is not supported.

2.1.22 [W3C-P3P1.0] Section 4, Compact Policies

V0030:

The specification states:

```
Compact policies are a performance optimization that is OPTIONAL for either user
agents or servers. User agents that are unable to obtain enough information from a
compact policy to make a decision according to a user's preferences SHOULD fetch
the full policy.
```

All Document Modes (All Versions)

No option is available to set privacy preferences that require downloading the full P3P policy file. However, end users can customize several actions on compact P3P policies by clicking the **Tools** menu, clicking **Internet Options**, clicking the **Privacy** tab, and then clicking **Import** to select the appropriate compact P3P policy file.

2.1.23 [W3C-P3P1.0] Section 5.5, Basic Data Structures

V0031:

The specification states:

```
All P3P-compliant user agent implementations MUST be aware of the Basic Data
Structures. Each table below specifies the elements of a basic data structure, the
categories associated, their structures, and the display names shown to users. More
than one category may be associated with a fixed data element. However, each base
data element is assigned to only one category whenever possible.
```

All Document Modes (All Versions)

P3P basic data structures are not supported. Policies are not validated against user preference.

2.1.24 [W3C-P3P1.0] Section 5.6.1, User Data

V0032:

The specification states:

```
User agent implementations may prefer to develop their own short display names
rather than using the concatenated names when displaying information for the user.
```

All Document Modes (All Versions)

Information from user-defined data structures is not displayed.

2.1.25 [W3C-P3P1.0] Section 5.6.2, Third Party Data

V0033:

The specification states:

User agents may offer to store multiple such thirdparty data sets and allow users to select the appropriate values from a list when necessary.

All Document Modes (All Versions)

No method is provided to store multiple third-party data sets or to provide users a way to select a data set.

2.2 Clarifications

The following subsections identify clarifications to recommendations made by [\[W3C-P3P1.0\]](#).

2.2.1 [W3C-P3P1.0] Section 2.2, Locating Policy Reference Files

C0001:

The specification states:

For a user agent to process the policy that applies to a given resource, it must locate the policy reference file for that resource, fetch the policy reference file, parse the policy reference file, fetch any required P3P policies, and then parse the P3P policy or policies.

All Document Modes (All Versions)

The policy reference file and its appropriate policies are downloaded and parsed, but the P3P policies themselves are not parsed.

2.2.2 [W3C-P3P1.0] Section 2.3.2.1.2, Wildcards in policy reference files

C0002:

The specification states:

Note that P3P user agents MAY ignore any URI pattern that does not conform to [URI].

All Document Modes (All Versions)

Invalid URIs are ignored.

C0003:

The specification states:

The wildcard character MAY be used in the INCLUDE and EXCLUDE elements, in the COOKIE-INCLUDE and COOKIE-EXCLUDE elements, and in the HINT element.

All Document Modes (All Versions)

Wildcards are supported only for the **INCLUDE** and **EXCLUDE** elements.

2.2.3 [W3C-P3P1.0] Section 2.3.2.3.3, Requesting Policies and Policy Reference Files

C0004:

The specification states:

Note that it is impossible for a client to accurately predict the amount of latency that may affect an HTTP request. Thus, if the policy reference file covering a request is going to expire soon, clients MAY wish to consider warning their users and/or revalidating the policy reference file before continuing with the request.

All Document Modes (All Versions)

Users are not warned if the P3P policy reference file is near expiration.

2.2.4 [W3C-P3P1.0] Section 2.3.4, Forms and Related Mechanisms

V0034:

The specification states:

User agents SHOULD NOT attempt to issue a HEAD request to an action URI if the relevant methods specified in the form's method attribute have been properly predeclared in the page's policy reference file.

All Document Modes (All Versions)

HEAD requests are never issued regardless of the methods that have been predeclared in the policy reference file of the webpage.

2.2.5 [W3C-P3P1.0] Section 2.4.1, Non-ambiguity

V0035:

The specification states:

If a user agent discovers more than one non-expired P3P policy for a given URI (for example because a page has both a P3P header and a link tag that reference different policy reference files, or because P3P headers for two pages on the site reference different policy reference files that declare different policies for the same URI), the user agent MAY assume any (or all) of these policies apply as the site MUST honor all of them.

All Document Modes (All Versions)

Only one policy for a given URI is recognized. The following ranking determines which policy applies:

1. The policy from the well-known location is given priority

2. The policy from the P3P header, if one exists and is different from the well-known location
3. The policy from the HTML link tag, if one exists and is different from both the well-known location and P3P header

2.2.6 [W3C-P3P1.0] Section 2.4.2, Multiple Languages

C0005:

The specification states:

Finally, language declarations can be also included directly within P3P XML files: the `POLICY`, `POLICIES`, `META`, and `DATASchema` elements MAY take an `xml:lang` attribute to indicate the language of any human-readable fields they contain (`xml:lang` is normatively defined in section 2.12 of [XML]).

All Document Modes (All Versions)

The **xml:lang** attribute is ignored, even if it is specified.

2.2.7 [W3C-P3P1.0] Section 2.4.8, Asynchronous Evaluation

C0006:

The specification states:

User agents MAY asynchronously fetch and evaluate P3P policies. That is, P3P policies need not necessarily be fetched and evaluated prior to other HTTP transactions. This behavior may be dependent on the user's preferences and the type of request being made. Until a policy is evaluated, the user agent SHOULD treat the site as if it has no privacy policy. Once the policy has been evaluated, the user agent SHOULD apply the user's preferences. To promote deterministic behavior, the user agent SHOULD defer application of a policy until a consistent point in time.

All Document Modes (All Versions)

Policies are downloaded only when the user requests to see the policy for a particular URI. To see policies, click the **Tools** menu, click **Internet Options**, and then click the **Privacy** tab.

2.2.8 [W3C-P3P1.0] Section 3.2.2, The **POLICY** element

C0007:

The specification states:

```
<POLICY>
  name (mandatory attribute)
  name of the policy, used as a fragment identifier to be able to reference the
  policy.
```

All Document Modes (All Versions)

The **name** attribute of the **POLICY** element is not required.

2.2.9 [W3C-P3P1.0] Section 3.6, User Preferences

C0008:

The specification states:

User agents MUST document a method by which preferences can be imported and processed, and SHOULD document a method by which preferences can be exported. P3P user agents MUST act according to the preference settings selected by the user.

All Document Modes (All Versions)

The following clarifications apply:

- No method is provided to export preferences.
- For sites that specify compact headers, only imported preferences are acted upon. Actions based on the data described in the full P3P policy are not blocked.

2.2.10 [W3C-P3P1.0] Section 4.1, Referencing compact policies

C0009:

The specification states:

```
compact-policy-field = `CP=` compact-policy ``  
  
compact-policy = compact-token *(" " compact-token)  
  
compact-token = compact-access |  
compact-disputes |  
compact-remedies |  
compact-non-identifiable |  
compact-purpose |  
compact-recipient |  
compact-retention |  
compact-categories |  
compact-test
```

All Document Modes (All Versions)

Users can define and import a custom privacy preference file that controls how both first-party and third-party cookies should be treated. For more information, see [http://msdn.microsoft.com/en-us/library/ms537344\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms537344(VS.85).aspx).

Users can specify any of the following operations for a cookie from a site (either first-party cookies or third-party cookies; with or without a compact P3P policy):

- Accept cookies.
- Reject cookies.
- **Prompt:** Prompts the user for consent.
- **forceFirstParty:** Leash cookies so that they are sent only in a first-party context.

- **forceSession:** Convert persistent cookies to session cookies.

The custom privacy file also allows users to define separate behaviors for first-party cookies and third-party cookies.

The custom privacy file supports rules (with actions) for each token on the compact P3P header. The action can be one of the operations in the previous list.

Example

```
<firstParty noPolicyDefault="accept" noRuleDefault="forceSession" alwaysAllowSession="no">  
<if expr="DSP" action="prompt"></if>  
</firstParty>
```

Therefore, the following compact policy tokens are supported:

Purposes:

- CURa, CURi, CURo
- ADMa, ADMi, ADMo
- DEVa, DEVi, DEVo
- CUSa, CUSi, CUSo
- TAIa, TAIi, TAIo
- PSAa, PSAi, PSAo
- PSDa, PSDi, PSDo
- IVAa, IVAi, IVAo
- IVDa, IVDi, IVDi
- CONa, CONi, CONo
- HISa, HISi, HISo
- TELa, TELi, TELo
- OTPa, OTPi, OTPo

Recipients:

- OURa, OURi, OURo
- DELa, DELi, DELo
- SAMa, SAMi, SAMo
- OTRa, OTRi, OTRo
- UNRa, UNRi, UNRo
- PUBa, PUBi, PUBo

Retention: NOR, STP, LEG, BUS, IND

Categories:

- PHY, ONL, UNI, PUR, FIN, COM, NAV, INT
- DEM, CNT, STA, POL, HEA, PRE, GOV, OTC

Nonidentifiable: NID

Disputes Section: DSP

Access: NOI, ALL, CAO, IDC, OTI, NON

Dispute Resolution: COR, MON, LAW

TST:Token for indicating that a policy is test-version: TST

2.2.11 [W3C-P3P1.0] Section 5.3, The DATA-DEF and DATA-STRUCT elements

C0010:

The specification states:

<DATA-DEF> and <DATA-STRUCT>

Define a data element or a data structure, respectively. Data structures are reusable structured type definitions that can be used to build data elements. Data elements are declared within a <STATEMENT> in a P3P policy to describe data covered by that statement.

The following attributes are common to these two elements:

name (mandatory attribute)

Indicates the name of the data element or data structure. Remember that names of data element and data structures are case-sensitive, so, for example, user.gender is different from USER.GENDER or User.Gender. Furthermore, in names of data elements and structures no number character can appear immediately following a dot. structref

URI reference ([URI]), where the fragment identifier part denotes the structure, and the URI part denotes the corresponding data schema where it is defined. The default base URI is a same-document reference ([URI]). Data elements or data structures without a structref attribute (and, so, without an associated structure) are called unstructured.

short-description

a string denoting the short display name of the data element or structure, no more than 255 characters.

The DATA-DEF and DATA-STRUCT elements can also contain a long description of the data element or structure, using the LONG-DESCRIPTION element.

All Document Modes (All Versions)

The **DATA-DEF** and **DATA-STRUCT** elements are not supported.

2.3 Error Handling

There are no additional considerations for error handling.

2.4 Security

There are no additional security considerations.

3 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

4 Index

A

[Asynchronous Evaluation](#) 22

B

[Basic Data Structures](#) 19

C

[Categories and the CATEGORIES element](#) 18

[Change tracking](#) 27

[Compact Policies](#) 19

E

Elements

[ACCESS](#) 12

[CATEGORIES](#) 18

[CONSEQUENCE](#) 14

[COOKIE-EXCLUDE](#) 10

[COOKIE-INCLUDE](#) 10

[DATA](#) 17

[DATA-STRUCT](#) 25

[DATE-GROUP](#) 17

[DISPUTES](#) 12

[ENTITY](#) 11

[EXCLUDE](#) 9

[EXTENSION](#) 18

[HINT](#) 9

[INCLUDE](#) 9

[LONG-DESCRIPTION](#) 12

[META](#) 8

[NON-IDENTIFIABLE](#) 14

[POLICIES](#) 11

[POLICY](#) 22

[POLICY-REFERENCES](#) 8

[PURPOSE](#) 15

[RECIPIENT](#) 15

[REMEDIES](#) 14

[RETENTION](#) 16

[Error handling for policy reference file and policy lifetimes](#) 9

[Extension Mechanism: the EXTENSION element](#) 18

F

Forms and Related Mechanisms ([section 2.1.7](#) 10, [section 2.2.4](#) 21)

G

[Glossary](#) 5

I

[Informative references](#) 5

[Introduction](#) 5

L

[Locating Policy Reference Files](#) 20

M

[Multiple Languages](#) 22

N

Non-ambiguity ([section 2.1.8](#) 11, [section 2.2.5](#) 21)

[Normative references](#) 5

R

References

[informative](#) 5

[normative](#) 5

[Referencing compact policies](#) 23

[Requesting Policies and Policy Reference Files](#) 21

T

[The ACCESS element](#) 12

[The CONSEQUENCE element](#) 14

[The COOKIE-INCLUDE and COOKIE-EXCLUDE elements](#) 10

[The DATA-DEF and DATA-STRUCT elements](#) 25

[The DATA-GROUP and DATA elements](#) 17

[The DISPUTES element](#) 12

[The ENTITY element](#) 11

[The HINT element](#) 9

[The INCLUDE and EXCLUDE elements](#) 9

[The META and POLICY-REFERENCES elements](#) 8

[The NON-IDENTIFIABLE element](#) 14

[The POLICIES element](#) 11

[The POLICY element](#) 22

[The PURPOSE element](#) 15

[The RECIPIENT element](#) 15

[The REMEDIES element](#) 14

[The RETENTION element](#) 16

[Third Party Data](#) 20

[Tracking changes](#) 27

U

[User Data](#) 19

[User Preferences](#) 23

W

Wildcards in policy reference files ([section 2.1.1](#) 8, [section 2.2.2](#) 20)