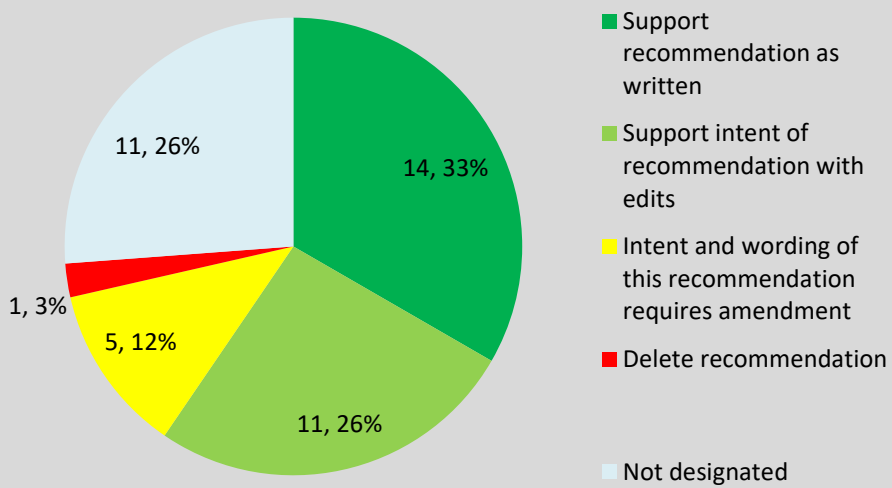
RECOMMENDATION 11 – Data Retention

#	Comment	Contributor	EPDP Response / Action Taken

The EPDP Team recommends that Registrars are required to retain the herein-specified data elements for a period of one year following the life of the registration. This retention period conforms to the specific statute of limitations within the Transfer Dispute Resolution Policy ("TDRP").



Support recommendation as written

#	Comment	Contributor	EPDP Response / Action Taken
1.	No comments provided in support of this recommendation	• John Poole; Domain Name Registrant • A. Mark Massey; Domain Name Rights Coalition • Evin Erdoğdu; ALAC • Greg Aaron; iThreat Cyber Group • Sivasubramanian Muthusamy; Internet Society India Chennai • Ben Butler; SSAC • Monica Sanders; i2Coalition • David Martel • Etienne Laurin	Support **EPDP Response:** The EPDP appreciates the support **Action Taken:** none [COMPLETED]
2.	Although difficult to quantify, 1 year of data retention period seems to be a reasonable period that it neither too less nor too high.	DR. JAIDEEP KUMAR MISHRA ; DIRECTOR MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA	Support **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
3.	Retaining the registration data for a year can help protect the rights of registrants and was seen as a legitimate purpose for data collection by contracted parties.	Ayden Férdeline; NCSG	Support **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
4.	We support the fact that a retention period is now substantiated with policy requirements, namely the TDRP. It shall be clarified, however, that data retained for that purpose may only be used for that purpose and not for other purposes. The purpose would cover escrowing data as that is also to ensure the legal position of the registered name holder according to the TDRP can be secured.	• Lars Steffen; eco – Association of the Internet Industry • Wolf-Ulrich Knoben; ISPCP Constituency	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
5.	Retaining the registration data for a year can help protect the rights of registrants and was seen as a legitimate purpose for data collection by contracted parties.	Farzaneh Badii; Internet Governance Project	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Support intent of recommendation with edits			
6.	No proposed edit or rationale was provided.	• Domain.com, LLC & affiliates • Brian King; MarkMonitor, Inc., a Clarivate Analytics company	Concerns **EPDP Response:** The EPDP takes note of the designation for "Support intent of recommendation with edits. **Action Taken:** none [**COMPLETED**]
7.	Change to: "The EPDP Team recommends that Registrars are required to retain the herein -specified data elements for a period of at least one year following the life of the registration…." We support the intent of this recommendation but would suggest the language be edited as noted above to allow for registrars to choose to retain data for longer than one year if applicable law or other guidance suggests longer than a one year data retention period.	• Zoe Bonython; RrSG • Volker Greimann; Key-Systems GmbH	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
8.	The EPDP Team recommends that Registrars are required to retain the herein specified data elements for a period of three years following the life of the registration. ICANN itself recommends a longer period of two years. Cybersecurity incidents have dwell time that can endure for years, as the recent Marriott/Starwood breach news proves. Attack indicators can be discovered long after the attack itself, and after DNS resources are deleted. Investigation timelines, particularly when it involves law enforcement, can be lengthy. It's important that information about previously registered domains is retained for a useful period for security and law enforcement needs -- one year simply is insufficient. The consistent utilization, by security and LEA personnel, of historic data from various third party Whois services is testament to the need.	Steve DelBianco; BC	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
9.	"The EPDP Team recommends that Registrars are required to retain the herein -specified data elements for a period of 3 years following the life of the registration." ICANN recommends a longer period (2 years) in the 2013 RAA. Although ICANN RAA may change as a result of the EPDP process, the point is worth noting. Although many investigations can proceed with data retained only one year after expiration, recent investigations reveal that some adversaries conduct subsequent attacks long after an attack has been concluded and that some attacks are only discovered after the event. Having a longer history of registrant data has also aided in proactive detection of new attacks by these previous attackers.	Jeremy Dallman, David Ladd – Microsoft Threat Intelligence Center; Amy Hogan-Burney, Richard Boscovich – Digital Crimes Unit; Makalika Naholowaa, Teresa Rodewald, Cam Gatta – Trademark; Mark Svancarek, Ben Wallace, Paul Mitchell – Internet Technology & Governance Policy; Cole Quinn – Domains and Registry; Joanne Charles – Privacy & Regulatory Affairs; Microsoft Corporation	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
10.	While we support the intent of this recommendation it is important to ensure that any retention period is lawful. This recommendation should be edited to allow for registrars to choose to retain data for longer than one year if applicable law or other guidance suggests longer than a one year data retention period.	Sara Bockey; GoDaddy	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
11.	The EPDP Team recommends that Registrars are required to retain the mandatory data elements for a period of one year following the life of the registration. ICANN must also commit to deleting this personal data after a period of one year following receipt of such data. Any "optional" data elements (such as the Technical contact may become) should be retained only while in use, and should be deleted once the data subject opts out of using that optional data. This retention period conforms to the specific statute of limitations within the Transfer Dispute Resolution Policy ("TDRP"). This data retention duration should apply to ICANN, the Registrar, and the Registry (if applicable). There is no need for ICANN to retain the herein specified mandatory data elements for longer than one year. Optional data should only be kept while the legal basis for processing remains active; if this legal basis is the data subject's consent to allow optional data use, then once that consent is revoked the data must no longer be retained.	Tucows Domains Inc.	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
12.	The RySG recommends editing Recommendation #11 as follows: "The EPDP Team recommends that Registrars are required to retain the herein -specified data elements for a period of one year following the life of the registration." The use of the term 'statute of limitations' is incorrect. Additionally the retention period should merely be set/stated, and not linked to a specific applicable requirement. The rationale as to why 1 year is set should be documented in full, but should not be included in the recommendation itself. The recommendation should not preclude any registrar from choosing to retain data for a longer period of time than 1 year, in accordance with their specific business needs and applicable laws For the avoidance of doubt, any additional retention periods which a registrar may see fit to implement, will be the sole responsibility of that registrar.	Wim Degezelle ; RySG	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
13.	The EPDP Team recommends that Registrars are required to retain the herein specified data elements for a period of three years following the life of the registration. ICANN itself recommends a longer period of 2 years. Cybersecurity incidents have dwell time that can go years, as the recent Marriott/Starwood breach news proves. Attack indicators can be discovered long after the attack itself, and after DNS resources are deleted. Investigation, particularly when it involves law enforcement, can be lengthy. It's important that information on previously registered domains is retained for a useful period for security and law enforcement needs. One year is simply not enough time for lookback needs. The consistent utilization, by security and LEA personnel, of historic data from various 3rd party Whois services is testament to the need.	Brian King; IPC	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
14.	The GAC notes that a number of Data protection laws call for retention periods to be only long enough as to carry out the lawful purposes. Within the EPDP process the members have noted the TDRP process requirements for at least the life of the domain plus one year to be able to fulfil its purposes. At least one year would typically be necessary to complete formal MLAT processes to request information from outside the requester's jurisdiction. ICANN's compliance team also indicated during the Los Angeles face to face meeting that the life of the domain plus one year would meet most of their investigation timeframes but a few requests would fall outside of this time frame. However, certain requests for information take place after the domain had been shut down. These requests may involve serious crimes or relate to significant cyber security risks and a one year data retention period would likely be insufficient under these circumstances as stated in the GAC Feedback on Proposed Interim Models (28 January 2018). The GAC requests that the EPDP team consider extending the period of retention of data when in receipt of a legitimate request.	Fabien Betremieux; GAC	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Intent and wording of this recommendation requires amendment			
15.	should be at least the 2 years recommended by ICANN, preferably longer. DomainTools knows how useful this data is and for how long, due to the actions of our security customers against our own historical Whois database. 1 year is not nearly long enough to support the legitimate interests outlined previously.	Tim Chen; DomainTools	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
16.	Make the minimum retention at least 6 years, consistent with various statute of limitations in the real world for crimes (property theft, etc.). The TDRP is not the only mechanism that exists for domain disputes. Courts can also be used (and for some crimes, there might not be any statute of limitation, and certainly longer than 1 year for property crimes). When domain name thefts/disputes occur, it's important to have a full audit trail of past WHOIS records, and the proposed policy would thwart that, because it would destroy data after 1 year of a registrar change (registrars often change when domains are stolen). Registrants should at a minimum be able to opt-in to a longer period, but the minimum period should be at least 6 years.	George Kirikos; Leap of Faith Financial Services Inc.	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
17.	The EPDP Team recommends that Registrars are required to retain the herein-specified data elements for a period of three years following the life of the registration. ICANN itself recommends a longer period of 2 years. Cybersecurity incidents have dwell time that can go years, as the recent Marriott/Starwood breach news proves. Attack indicators can be discovered long after the attack itself, and after DNS resources are deleted. Investigation, particularly when it involves law enforcement, can be lengthy. It's important that information on previously registered domains is retained for a useful period for security and law enforcement needs. One year is simply not enough time for lookback needs. The consistent utilization, by security and law enforcement personnel, of historic data from various third party Whois services is testament to the need.	Dean S. Marks; Coalition for Online Accountability	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
18.	The AG IS believes that the EPDP proposed one year data retention period is insufficient for important cybersecurity purposes that, like other legitimate interests, must be considered beyond use for Transfer Dispute Resolution Policy purposes. Offenders, including those responsible for significant security threats, inadvertently reveal crucial identifiers, often at the beginning of their career but also over time. Likewise, changes in a Whois record over the course of years provides important insight into not only cybersecurity investigations but also prevention of future attacks through correlation analysis. Consequently, the analysis of historical Whois data is part and parcel of most cybersecurity investigations. Over the years, there have been many examples of botnets, DDoS attacks, malware hosting, SPAM, and phishing campaigns that have been successfully uncovered because of Whois record correlation with data points older than a year. For example, the perpetrator of a 2016 Mirai botnet offshoot attack on approximately a million Deutsche Telekom routers in Germany was discovered using historical Whois data that predated the attack by several years. Accordingly, it is important to not only retain the most recent registration record but also all registration history for a long period of time. Recent examples suggest at least six years is necessary.	Greg Mounier on behalf of Europol AGIS; Europol Advisory Group on Internet Security	Concerns **EPDP Response:** The EPDP considered the designation of "Intent and wording of this recommendation requires amendment" **Action Taken:** none [**COMPLETED**]
19.	Further to our observations on ICANN's request for feedback on Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the GDPR, a one-year data retention practice would risk harming legitimate investigations. ICANN may recall that other industries' (e.g., accounting and legal) data retention best practices generally point to seven years as a guide. (See e.g., www.sec.gov/rules/final/33-8180.htm, and www.vantageinsurance.co.uk/assets/files/atrisk/September%202011.pdf.)	Brian Beckham; Head, Internet Dispute Resolution Section at WIPO	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Delete recommendation			

#	Comment	Contributor	EPDP Response / Action Taken
20.	Language needs to be added to cater for data retention waivers	Michele Neylon; Blacknight Internet Solutions Ltd	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Not designated			
21.	No selection made and no additional comments submitted	• Lori Schulman Senior Director, Internet Policy; International Trademark Association (INTA) • Neil Fried; The Motion Picture Association of America • Steve Gobin; Corporate domain name management • Ashley Heineman; NTIA • Sajda Ouachtouki; The Walt Disney Company • Monique A. Goeschl; Verein für Anti-Piraterie der Film- und Videobranche (VAP) • Theo Geurts • Ivett Paulovics; MFSD Srl URS Provider • Ashley Roberts; Valideus • Renee Fossen; Forum - URS and UDRP Provider • Stephanie Perrin	**EPDP Response:** none **Action Taken:** none [**COMPLETED**]

RECOMMENDATION 11 – Additional Comments

#	Comment	Contributor	EPDP Response / Action Taken

#	Comment	Contributor	EPDP Response / Action Taken
22.	Further to our observations on ICANN's request for feedback on Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the GDPR, a one-year data retention practice would risk harming legitimate investigations. ICANN may recall that other industries' (e.g., accounting and legal) data retention best practices generally point to seven years as a guide. (See e.g., www.sec.gov/rules/final/33-8180.htm, and www.vantageinsurance.co.uk/assets/files/atrisk/September%202011.pdf.)	Brian Beckham; Head, Internet Dispute Resolution Section at WIPO	New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
23.	ICANN recommends a longer period, 2 years. Cybersecurity incidents have dwell time that can go years, as recent breach news proves. Attack indicators can be discovered long after the attack itself, and after DNS resources are deleted. Investigation, particularly when it involves law enforcement, can be lengthy. It's important that information on previously registered domains is retained for a useful period for security and law enforcement needs. One year is not enough time for lookback needs. The consistent utilization, by security and LEA personnel, of historic data from various 3rd party WHOIS services is testament to the need.	Brian King; MarkMonitor, Inc., a Clarivate Analytics company	New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
24.	The RySG cautions the over reliance on just identifying the limitation for the TDRP. Note that if a retention period is specifically linked to data retained for a specific purpose, data retained beyond the minimum, may ONLY be used for that purpose. Whereas we completely encourage the identification of the necessity for different limitation periods, thus linking retention to specific and measurable periods, the ePDP should compile all specific grounding limitation periods to ensure the ongoing use for such purposes. Furthermore, the IRTP Policy Status Report is currently out for public comment and could lead to work that changes the TDRP retention period.	Wim Degezelle ; RySG	New Idea **EPDP Response:** refer to like comments above in the "yes/no" sections **Action Taken:** none [**COMPLETED**]
25.	The GAC requests that the EPDP team consider extending the period of retention of data when in receipt of a legitimate request.	Fabien Betremieux; GAC	New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
26.	Although difficult to quantify, 1 year of data retention period seems to be a reasonable period that it neither too less nor too high.	DR. JAIDEEP KUMAR MISHRA ; DIRECTOR MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA	New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]