# BUSINESS CONSTITUENCY

NIS 2 INPUT FOR THE FRENCH COUNCIL PRESIDENCY

---

*ENSURING WHOIS DATA ACCESS THAT SUPPORTS CYBERSECURITY, LAW ENFORCEMENT, AND RESPONSIBLE BUSINESS ON THE INTERNET*

Dear Ambassador Dubreuil:

We are writing to you to express our support for the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, better known as *NIS 2*. We applaud the work of the Commission, the Parliament, and the Council to develop the NIS 2 directive, as tripartite negotiations will soon begin in earnest. We hope we can be a resource as this initiative advances and we would like to provide our views on some components that are critical to the Business Constituency (BC) of ICANN, the not-for-profit public-benefit corporation dedicated to keeping the Internet secure, stable and interoperable.

The BC is the voice of commercial Internet users within ICANN, representing the interests of small, medium, large and multinational enterprises as users of the Domain Name System (DNS). Business users, often the target of nefarious DNS activity and thus deeply invested in abuse mitigation, have been an active voice in the multi-stakeholder community that plays a critical role in addressing DNS abuse.

We would like to express unequivocal support for NIS 2 and the objectives of policymakers seeking to advance cybersecurity by improving the Union's strategic autonomy, collective response, and resilience in the context of a global and open Internet. The initiative represents a major improvement on the current cybersecurity Directive as it is responsive to evolving threats and supportive of the needs of technical experts with everyday experience in keeping the Internet safe and mitigating cybersecurity risks.

# BUSINESS CONSTITUENCY

The BC views certain elements of NIS 2 as much-needed legislative support for, and clarification of, the critical functions of Internet infrastructure, including the DNS. The inclusion of provisions to uphold and preserve a reliable, resilient and secure DNS are prime examples of the sophistication and importance of NIS 2, which rightly recognizes and effectively identifies the broad range of stakeholders that play a role in the security and operations of the DNS, including 'domain name registration services' like registries and registrars, privacy or proxy registration service providers, and domain brokers or resellers.

NIS 2 also makes clear the critical value of the WHOIS database and legitimate access to the information therein, which is essential to identifying *who is* behind an abusive domain name or website. This information has been a tool for public safety, law enforcement and other authorities in their effort to protect consumers on the Internet from cybersecurity attacks, sexual trafficking and exploitation, fraud and counterfeited products, and other harms or threats.

WHOIS data access issues have proven to be a difficult hurdle for ICANN policymaking in recent years. Changes to WHOIS access following ICANN's questionable interpretations of GDPR and its temporary specification for global Top Level Domain (TLD) registration data continue to significantly impede cybersecurity applications and forensic investigations, propagating harm and loss to the many Internet users that are victims of phishing, malware or other cyber attacks.

Article 23 in the draft Directive provides helpful clarification of the relation between WHOIS data and GDPR requirements, properly applies the obligations for processing and publication of WHOIS data to registrars and registries, and rightfully recognizes the critical parts these entities play in enabling access to WHOIS data. Retaining and further clarifying these points will only strengthen the Directive. NIS 2 can also provide long sought-after clarity on the specific WHOIS data elements that must be made publicly accessible, and on the legal obligations of domain name registration services to grant access to the data to legitimate access seekers.

# BUSINESS CONSTITUENCY

**Members of the ICANN Business Constituency, along with law enforcement officials and other stakeholder groups, had long depended on WHOIS information as an essential tool to prevent and enforce against a wide range of illegal activity that continues to be a direct threat to the safety and wellbeing of Internet users. NIS 2 is an opportunity to restore the value of the WHOIS database for the Internet community. To achieve this goal, the final Directive should include three critical requirements of Top Level Domain registries and entities providing domain name registration services:**

1. **that they collect and maintain accurate, verified and complete domain name registration data;**

2. **that they make non-personal WHOIS data publicly available without undue delay; and**

3. **that they provide access to specific domain name registration data, including personal data, upon duly justified requests of legitimate access seekers.**

**Supporting mechanisms and recitals in the Directive can clarify a high standard for verification of accurate domain name registration data and ensure that the rights of legitimate access seekers extend to stakeholder groups involved in the prevention and detection of crime, fraud, and other DNS abuse.**

We applaud the effort to include these elements in the approaches to the NIS 2 Directive that have been developed thus far and urge the relevant stakeholders to preserve them in the upcoming trilogue negotiations. We would like to make our group available as a resource to provide input on these matters that are critical to the transparency and utility of WHOIS data, a vitally important tool for the safety and wellbeing of Internet users.

# BUSINESS CONSTITUENCY

NIS 2 INPUT FOR DG CONNECT

---

*ENSURING WHOIS DATA ACCESS THAT SUPPORTS CYBERSECURITY, LAW ENFORCEMENT, AND RESPONSIBLE BUSINESS ON THE INTERNET*

Dear Director General Viola:

We are writing to you to express our support for the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, better known as *NIS 2*. We applaud the work of the Commission, the Parliament, and the Council to develop the NIS 2 directive, as tripartite negotiations will soon begin in earnest. We hope we can be a resource as this initiative advances and we would like to provide our views on some components that are critical to the Business Constituency (BC) of ICANN, the not-for-profit public-benefit corporation dedicated to keeping the Internet secure, stable and interoperable.

The BC is the voice of commercial Internet users within ICANN, representing the interests of small, medium, large and multinational enterprises as users of the Domain Name System (DNS). Business users, often the target of nefarious DNS activity and thus deeply invested in abuse mitigation, have been an active voice in the multi-stakeholder community that plays a critical role in addressing DNS abuse.

We would like to express unequivocal support for NIS 2 and the objectives of policymakers seeking to advance cybersecurity by improving the Union's strategic autonomy, collective response, and resilience in the context of a global and open Internet. The initiative represents a major improvement on the current cybersecurity Directive as it is responsive to evolving threats and supportive of the needs of technical experts with everyday experience in keeping the Internet safe and mitigating cybersecurity risks.

# BUSINESS CONSTITUENCY

The BC views certain elements of NIS 2 as much-needed legislative support for, and clarification of, the critical functions of Internet infrastructure, including the DNS. The inclusion of provisions to uphold and preserve a reliable, resilient and secure DNS are prime examples of the sophistication and importance of NIS 2, which rightly recognizes and effectively identifies the broad range of stakeholders that play a role in the security and operations of the DNS, including 'domain name registration services' like registries and registrars, privacy or proxy registration service providers, and domain brokers or resellers.

NIS 2 also makes clear the critical value of the WHOIS database and legitimate access to the information therein, which is essential to identifying *who is* behind an abusive domain name or website. This information has been a tool for public safety, law enforcement and other authorities in their effort to protect consumers on the Internet from cybersecurity attacks, sexual trafficking and exploitation, fraud and counterfeited products, and other harms or threats.

WHOIS data access issues have proven to be a difficult hurdle for ICANN policymaking in recent years. Changes to WHOIS access following ICANN's questionable interpretations of GDPR and its temporary specification for global Top Level Domain (TLD) registration data continue to significantly impede cybersecurity applications and forensic investigations, propagating harm and loss to the many Internet users that are victims of phishing, malware or other cyber attacks.

Article 23 in the draft Directive provides helpful clarification of the relation between WHOIS data and GDPR requirements, properly applies the obligations for processing and publication of WHOIS data to registrars and registries, and rightfully recognizes the critical parts these entities play in enabling access to WHOIS data. Retaining and further clarifying these points will only strengthen the Directive. NIS 2 can also provide long sought-after clarity on the specific WHOIS data elements that must be made publicly accessible, and on the legal obligations of domain name registration services to grant access to the data to legitimate access seekers.

# BUSINESS CONSTITUENCY

**Members of the ICANN Business Constituency, along with law enforcement officials and other stakeholder groups, had long depended on WHOIS information as an essential tool to prevent and enforce against a wide range of illegal activity that continues to be a direct threat to the safety and wellbeing of Internet users. NIS 2 is an opportunity to restore the value of the WHOIS database for the Internet community. To achieve this goal, the final Directive should include three critical requirements of Top Level Domain registries and entities providing domain name registration services:**

1. **that they collect and maintain accurate, verified and complete domain name registration data;**

2. **that they make non-personal WHOIS data publicly available without undue delay; and**

3. **that they provide access to specific domain name registration data, including personal data, upon duly justified requests of legitimate access seekers.**

**Supporting mechanisms and recitals in the Directive can clarify a high standard for verification of accurate domain name registration data and ensure that the rights of legitimate access seekers extend to stakeholder groups involved in the prevention and detection of crime, fraud, and other DNS abuse.**

We applaud the effort to include these elements in the approaches to the NIS 2 Directive that have been developed thus far and urge the relevant stakeholders to preserve them in the upcoming trilogue negotiations. We would like to make our group available as a resource to provide input on these matters that are critical to the transparency and utility of WHOIS data, a vitally important tool for the safety and wellbeing of Internet users.

# BUSINESS CONSTITUENCY

NIS 2 INPUT FOR THE EUROPEAN PARLIAMENT

---

*ENSURING WHOIS DATA ACCESS THAT SUPPORTS CYBERSECURITY, LAW ENFORCEMENT, AND RESPONSIBLE BUSINESS ON THE INTERNET*

Dear Mr Groothuis, MEP:

We are writing to you to express our support for the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, better known as *NIS 2*. We applaud the work of the Commission, the Parliament, and the Council to develop the NIS 2 directive, as tripartite negotiations will soon begin in earnest. We hope we can be a resource as this initiative advances and we would like to provide our views on some components that are critical to the Business Constituency (BC) of ICANN, the not-for-profit public-benefit corporation dedicated to keeping the Internet secure, stable and interoperable.

The BC is the voice of commercial Internet users within ICANN, representing the interests of small, medium, large and multinational enterprises as users of the Domain Name System (DNS). Business users, often the target of nefarious DNS activity and thus deeply invested in abuse mitigation, have been an active voice in the multi-stakeholder community that plays a critical role in addressing DNS abuse.

We would like to express unequivocal support for NIS 2 and the objectives of policymakers seeking to advance cybersecurity by improving the Union's strategic autonomy, collective response, and resilience in the context of a global and open Internet. The initiative represents a major improvement on the current cybersecurity Directive as it is responsive to evolving threats and supportive of the needs of technical experts with everyday experience in keeping the Internet safe and mitigating cybersecurity risks.

# BUSINESS CONSTITUENCY

The BC views certain elements of NIS 2 as much-needed legislative support for, and clarification of, the critical functions of Internet infrastructure, including the DNS. The inclusion of provisions to uphold and preserve a reliable, resilient and secure DNS are prime examples of the sophistication and importance of NIS 2, which rightly recognizes and effectively identifies the broad range of stakeholders that play a role in the security and operations of the DNS, including 'domain name registration services' like registries and registrars, privacy or proxy registration service providers, and domain brokers or resellers.

NIS 2 also makes clear the critical value of the WHOIS database and legitimate access to the information therein, which is essential to identifying *who is* behind an abusive domain name or website. This information has been a tool for public safety, law enforcement and other authorities in their effort to protect consumers on the Internet from cybersecurity attacks, sexual trafficking and exploitation, fraud and counterfeited products, and other harms or threats.

WHOIS data access issues have proven to be a difficult hurdle for ICANN policymaking in recent years. Changes to WHOIS access following ICANN's questionable interpretations of GDPR and its temporary specification for global Top Level Domain (TLD) registration data continue to significantly impede cybersecurity applications and forensic investigations, propagating harm and loss to the many Internet users that are victims of phishing, malware or other cyber attacks.

Article 23 in the draft Directive provides helpful clarification of the relation between WHOIS data and GDPR requirements, properly applies the obligations for processing and publication of WHOIS data to registrars and registries, and rightfully recognizes the critical parts these entities play in enabling access to WHOIS data. Retaining and further clarifying these points will only strengthen the Directive. NIS 2 can also provide long sought-after clarity on the specific WHOIS data elements that must be made publicly accessible, and on the legal obligations of domain name registration services to grant access to the data to legitimate access seekers.

# BUSINESS CONSTITUENCY

**Members of the ICANN Business Constituency, along with law enforcement officials and other stakeholder groups, had long depended on WHOIS information as an essential tool to prevent and enforce against a wide range of illegal activity that continues to be a direct threat to the safety and wellbeing of Internet users. NIS 2 is an opportunity to restore the value of the WHOIS database for the Internet community. To achieve this goal, the final Directive should include three critical requirements of Top Level Domain registries and entities providing domain name registration services:**

1. **that they collect and maintain accurate, verified and complete domain name registration data;**

2. **that they make non-personal WHOIS data publicly available without undue delay; and**

3. **that they provide access to specific domain name registration data, including personal data, upon duly justified requests of legitimate access seekers.**

**Supporting mechanisms and recitals in the Directive can clarify a high standard for verification of accurate domain name registration data and ensure that the rights of legitimate access seekers extend to stakeholder groups involved in the prevention and detection of crime, fraud, and other DNS abuse.**

We applaud the effort to include these elements in the approaches to the NIS 2 Directive that have been developed thus far and urge the relevant stakeholders to preserve them in the upcoming trilogue negotiations. We would like to make our group available as a resource to provide input on these matters that are critical to the transparency and utility of WHOIS data, a vitally important tool for the safety and wellbeing of Internet users.