

GPEN Alert

A Secure Information-Sharing System for the Global Privacy Enforcement Network

In June 2007, the Organization for Economic Cooperation and Development (OECD) adopted a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy (Recommendation). The Recommendation provided that “[m]ember countries should foster the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns.” The Recommendation also provided that privacy enforcement authorities “should co-operate with each other, consistent with the provisions of this Recommendation and national law, to address cross-border aspects arising out of the enforcement of Laws Protecting Privacy.”

Building upon this Recommendation, eleven privacy enforcement authorities joined together to establish the Global Privacy Enforcement Network (GPEN) in March 2010 and to adopt an Action Plan. The Action Plan identifies GPEN’s mission as connecting privacy enforcement authorities from around the world to promote and support cooperation in cross-border enforcement of laws protecting privacy.

At the October 2011 GPEN meeting in Mexico City, GPEN members decided to explore the development of a secure online information-sharing tool for GPEN members to facilitate cooperation and coordination in specific cross-border investigations and enforcement matters. The United States Federal Trade Commission (FTC) has made available the “Consumer Sentinel Network” (CSN) as the platform on which to build this GPEN information-sharing tool – the “GPEN Alert” system.

The Consumer Sentinel Network

The FTC, in conjunction with various other government and private organizations, developed the CSN, a secure, non-public, online database maintained by the FTC that stores consumer complaint data and other investigatory information provided by consumers, participating domestic and international law enforcement agencies, and other contributors about consumer fraud and deception.

GPEN Alert

GPEN Alert is intended to be a separate information-sharing tool for GPEN members that uses the secure CSN platform infrastructure and user interface, but is otherwise segregated from the CSN database. Initially, participating privacy enforcement authorities may use GPEN Alert to notify other member authorities of their privacy investigations and enforcement actions, particularly those that have cross-border aspects, for purposes of potential coordination and cooperation. In the future, GPEN Alert functions may be expanded to allow the sharing of additional confidential, non-public enforcement information relating to specific investigations and enforcement matters, and/or to allow the sharing of consumer complaints relating to privacy.

In any case, it remains to each member authority to decide what information they will input, share, and access via GPEN Alert according to their own domestic regimes.

When adding information to GPEN Alert, a member authority is able to select whether all other members or a specified subset of members can view the information by selecting from a list of member authorities and other groupings to be implemented (“International Conference members,” “APEC CPEA Members” etc...).

Specifically, GPEN Alert members may use this secure tool to (1) alert other members about investigations and law enforcement matters and (2) find out whether other members are investigating or taking enforcement actions against the same company, person or practices. Information may be contributed and accessed only by GPEN member authorities that have signed the Memorandum of Understanding (MOU) and whose relevant staff have individual accounts with multifactor authentication (See the MOU’s Appendix). Additionally, Participants must execute the separate Data Security and Minimum Safeguards Certification for Access to GPEN Alert Information before they can access GPEN Alert.

GPEN Committee members who participate in this MOU are to make strategic decisions regarding GPEN Alert. A Joint Oversight Panel (JOP) of three GPEN members who participate in this MOU will perform operational duties of running GPEN Alert. The FTC, which operates and maintains GPEN Alert, may suspend or limit access by current Participants where necessary to protect the security and operational integrity of the system or other systems operated by the FTC.

MULTILATERAL MEMORANDUM OF UNDERSTANDING FOR PARTICIPATION IN THE “GPEN ALERT” SYSTEM

Preamble

The signatories of this Memorandum of Understanding (“MOU”),

RECOGNISING that modern commerce and communications increasingly rely on the seamless flow of personal information across borders, and that these global data flows occur across jurisdictions having a wide diversity of privacy laws and enforcement arrangements;

RECOGNISING the challenges posed by cross-border flows of personal data;

RECOGNISING the desirability of more effective cross-border enforcement of privacy and data security laws and regulations;

RECOGNISING the desirability of enhancing confidence in cross-border data flows, and of preventing harm that can result from privacy and data security violations;

RECOGNISING that GPEN was created to strengthen personal privacy protections in this global context by assisting public authorities with responsibilities for enforcing domestic privacy laws to strengthen their capacities for cross-border cooperation;

RECOGNISING that other international organizations and networks, such as the OECD, the International Conference of Data Protection and Privacy Commissioners, and several regional networks have called for and taken practical steps to improve international privacy enforcement cooperation;

RECOGNISING that the International Conference of Data Protection and Privacy Commissioners has called for the development of an international secure information platform that offers a “safe space” for privacy enforcement authorities to share confidential information and to facilitate the initiation and conduct of coordinated enforcement action;

RECOGNISING that this Memorandum of Understanding does not impose legal commitments on the Participants, and that nothing in this Memorandum of Understanding requires Participants to participate or provide support in a manner inconsistent with their respective national laws, law enforcement policies, or other important interests, or to cooperate or share information with any other Participant in this Memorandum of Understanding on any given matter,

HAVE REACHED THE FOLLOWING UNDERSTANDING:

1. Definitions

This MOU uses the following definitions:

- A. “Participant(s)” refers to GPEN members that are signatories to this MOU, and may also include former Participants with respect to continuing confidentiality and data security commitments.
- B. “Specified Participant(s)” refers to one or more Participants that have been granted access to view contributed GPEN Alert Information by the Participant that contributed the information.
- C. “Consumer Sentinel Network” or “CSN” refers to a secure, non-public, online database maintained by the U.S. Federal Trade Commission (“FTC”) that stores consumer complaint data and other investigatory information provided by consumers, participating law enforcement agencies, and other contributors about consumer fraud and deception.
- D. “GPEN Alert” refers to the secure online information-sharing tool operated and maintained by the FTC built onto the CSN platform as a separate service for GPEN members that have signed this Memorandum of Understanding.
- E. “GPEN Committee” refers to the GPEN Committee designated under the GPEN Action Plan.
- F. “Joint Oversight Panel” or “JOP” refers to a three-Participant panel (that includes the FTC as the operator of CSN and GPEN Alert) that assists the FTC with the implementation and operation of GPEN Alert system and that performs the functions set out in paragraph 6 of this MOU.
- G. “Privacy Enforcement Authority” refers to a public privacy enforcement authority that: (1) is responsible for enforcing laws or regulations the enforcement of which has the effect of protecting personal data; and (2) is empowered to conduct investigations or pursue enforcement proceedings.
- H. “GPEN Alert Information” refers to information contributed by Participants that identifies the targets and subject matters of their ongoing or anticipated investigations or enforcement actions, including the existence of such investigations, to facilitate coordination and cooperation with other Participants that are interested in the same targets.

2. Purpose and Use

This MOU is entered into by the Participants for the purpose of facilitating the confidential exchange of information through GPEN Alert relating to ongoing or anticipated investigations or enforcement matters that have cross-border aspects, so that Participants can coordinate and cooperate with one another where desired, appropriate and permitted by their respective domestic laws.

3. Access to GPEN Alert Information

Participants intend for GPEN Alert Information to be available only to other Participants or to Specified Participants as indicated by the providing Participant. Participants are to have access only to GPEN Alert Information through this MOU, not to other CSN information. Staff of GPEN Alert Participants are to receive accounts with CSN usernames, passwords, and multifactor authentication that provides Participants with access only to GPEN Alert Information.

4. Confidentiality and Use of GPEN Alert Information

All Participants intend to keep all GPEN Alert Information contributed by other Participants confidential. This confidentiality applies not only to the GPEN Alert Information, but also to the existence of an investigation to which the GPEN Alert Information relates.

The Participants intend to use the GPEN Alert Information to which they have access under paragraph 3 of this MOU only in connection with ongoing or anticipated investigations or enforcement actions relating to data protection or privacy.

Except as required or authorized by law, otherwise set forth in this MOU, or otherwise decided with or specified by the Participant contributing information, Participants intend not to release information obtained through GPEN Alert, or provided to GPEN Alert by other Participants, to anyone other than their employees, consultants, and contractors or other bona fide personnel who have a need to know such information and who are bound to maintain such confidentiality. Participants understand that some Participants may have domestic statutory requirements that information may only be shared, including through GPEN Alert, with an expectation that it be treated in a confidential manner and not be further disclosed without the express consent of the Participant who provided the information.

If Participants receive a request for access to any GPEN Alert Information or should that information become subject to legal process, they are to immediately notify the provider of the requested information so that appropriate steps can be taken, and decisions made including, if appropriate, a timely decision on whether to furnish the requested information and, if the information is to be furnished, how to furnish it in a manner aimed at preserving its confidentiality.

If a Participant receives an enforceable request from another law enforcement agency or other governmental entity or is directed to furnish information in GPEN Alert to a non-Participant by a court of competent jurisdiction, the Participant may furnish that information subject to applicable statutory restrictions and in a manner that seeks to preserve the confidentiality of that information. In accordance with the previous paragraph, Participants are to immediately notify the provider of the request for information.

The Joint Oversight Panel may, by consensus, suspend or limit access to information in GPEN Alert if they have reason to believe a Participant has acted inconsistently with the expectations reflected in this MOU. In addition, it is understood that the FTC in its capacity as the operator of GPEN Alert may suspend or limit access by Participants to protect the security and operational integrity of the system, and it is expected that the FTC would provide notice

where practicable and appropriate.

5. Scope of Participation

The Participants intend to:

- A. develop and maintain a non-public, confidential and secure Website and information-sharing tool called “GPEN Alert” built onto the FTC’s CSN that can be accessed only by Participants;
- B. contribute as much GPEN Alert Information to GPEN Alert as appropriate and as is consistent with their laws, policies, enforcement priorities and resources;
- C. make reasonable efforts to provide GPEN Alert Information that is accurate and relevant for the purpose of facilitating cooperation among Participants;
- D. reimburse the FTC for multifactor authentication and other fees related to maintenance of user accounts for the tool, as specified in the Appendix;
- E. satisfy the data security safeguards requirements, which are not a part of this MOU, for access to GPEN Alert; and
- F. encourage other GPEN members to become Participants.

6. Joint Oversight Panel & The GPEN Committee

The JOP consists of the FTC as the operator of CSN and GPEN Alert, and two other Participants appointed by the GPEN Committee. The JOP performs operational duties of running GPEN Alert while the GPEN Committee makes strategic decisions concerning GPEN Alert. When the GPEN Committee is considering a matter involving GPEN Alert, only GPEN Committee members who are participants in GPEN Alert are to take part in that consideration.

The JOP has the following functions:

- A. Receive, review and decide on by consensus applications for participation in GPEN Alert system. (An application form is available on the GPEN website.)
- B. Review the status of current Participants that may no longer qualify for participation, or of Participants that may have acted inconsistently with the expectations reflected in the MOU (in cases where the FTC as the operator of GPEN Alert has not limited the Participant’s access to protect the security and operational integrity of the system as addressed in paragraph 4), and to decide (by consensus) on whether to suspend or limit access by such Participant.
- C. Consider and recommend to the GPEN Committee future changes and expansions of GPEN Alert functions, with the expectation that the JOP would consult with Participants

and publicize these recommendations via the GPEN Committee.

- D. Perform any other functions related to GPEN Alert as requested by the Participants or by the GPEN Committee.

7. Hosting GPEN Alert

The FTC is to use best efforts to:

- A. host and maintain GPEN Alert as a separate part of the FTC's CSN;
- B. make GPEN Alert available to Participants consistent with the data security and safeguards requirements, and the decisions of the GPEN Committee and the Joint Oversight Panel, as outlined in this MOU; and
- C. delete GPEN Alert Information that is more than one year old unless it has been removed or renewed by the providing Participant.

8. Duration of Participation

Participants intend to provide 60 days written notice to the JOP if they are ending their participation under this MOU. If a Participant ends their participation in this MOU, the Participant is to continue to maintain the confidentiality of any GPEN Alert information in its possession or control in accordance with Paragraph 4 and the data security and safeguards requirements.

9. Legal Effect

This MOU and its Appendix do not create any legally binding obligations by or amongst the Participants. In Particular, nothing in this MOU or its Appendix creates an obligation for Participants to provide information or cooperate in particular cases or with any particular other Participant. Participation pursuant to this MOU remains subject to the domestic laws and international obligations applicable to Participants. Any investigatory and enforcement cooperation following information sharing and coordination through GPEN Alert is subject to the applicable laws in the jurisdictions involved and any other arrangements between or amongst the cooperating Participants.

This MOU is not intended to create any rights on the part of any private person.

**SIGNATURE PAGE FOR THE
MULTILATERAL MEMORANDUM OF UNDERSTANDING FOR PARTICIPATION
IN THE “GPEN ALERT” SYSTEM**

Members of GPEN may become Participants in GPEN Alert by signing this MOU.

Signed:

Date:

Name:

Title:

Signed:

Date:

Name:

Title:

Signed:

Date:

Name:

Title:

APPENDIX

GPEN Alert User Account Operating Costs

GPEN Alert is built on the secure infrastructure, user interface, and authentication of the Consumer Sentinel Network (CSN) platform. Access to CSN is strictly controlled and uses unique user names, passwords, multifactor login authentication, approved IP address ranges, and security safeguards that the FTC has determined are necessary to ensure the confidentiality and security of the system and its data.

Participants understand that to provide this secure infrastructure:

1. Participant staff members can access GPEN Alert with individual accounts that use multifactor authentication.
2. Participants are to reimburse the FTC US \$150 for each of these accounts with multifactor authentication.

The payment allows the FTC to recover some of the cost of providing the accounts with multifactor authentication. It includes the costs for multifactor authentication, customer support, and agency requests to change the valid IP address lists and domain names.

The reimbursement covers accounts through November 30, 2021, and reimbursement amounts may be revised following that date.