VATRUS
VATEUR Division

VATRUS

Политика в отношении защиты и обработки данных

Data Protection And Handling Policy

Редакция 1.0 / Revision 1.0

21.01.2019

TABLE OF CONTENTS | ОГЛАВЛЕНИЕ

DOCUMENT IDENTIFICATION | ОПИСАНИЕ ДОКУМЕНТА

Type **Тип**	Policy Политика
Version **Версия**	1.0
Issue date **Дата создания**	10.01.2019
Effective date **Дата утверждения**	21.01.2019
Prepared by **Подготовил**	VATRUS7 Kirill Shabunin / Кирилл Шабунин
Approved by **Утвержден**	VATRUS1 Evgeny Vygornitsky / Евгений Выгорницкий
Review date **Дата проверки**	No later than 10.01.2022 Не позже 10.01.2022
Identification **Идентификационный номер**	VATRUS-POL-202_Data Protection And Handling Policy

REVISION RECORDS | ИСТОРИЯ ИЗМЕНЕНИЙ

Revision number Номер редакции	Description of change Описание изменений	Effective date Дата утверждения
1.0	Initial revision Документ введен впервые	21.01.2019

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119;

VATSIM refers to the organisation at https://www.vatsim.net/;

VATRUS refers to the organisation at https://www.vatrus.info/.

Ключевые слова “обязан”, “требуется” соответствуют пункту 1 стандарта RFC 2119;

Ключевое слово “не обязан” соответствует пункту 2 стандарта RFC 2119;

Ключевые слова “должен”, “рекомендуется” соответствуют пункту 3 стандарта RFC 2119;

Ключевые слова “не должен”, “не рекомендуется” соответствуют пункту 4 стандарта RFC 2119;

Термин VATSIM относится к организации на https://www.vatsim.net/;

Термин VATRUS относится к организации на https://www.vatrus.info/.

This document defines the VATRUS policy regarding the data protection and handling.

This Policy has been put in place to achieve the following aims:

- to comply with the law, particularly the EU General Data Protection Regulation;
- to ensure good data protection practice which when followed aims to protect members, staff, the organisation and other individuals using our services.

Настоящий документ определяет политику VATRUS в отношении защиты и обработки данных.

Настоящая политика была введена в действие для достижения следующих целей:

- соблюдать закон, в частности, общие положения о защите данных в ЕС;
- обеспечить надлежащую практику защиты данных, которая, при ее соблюдении, направлена на защиту участников, персонала, организации и других лиц, пользующихся нашими сервисами.

VATRUS collects a range of personal data on members, both provided by the members directly and from third parties.

While a member is using VATRUS services, or when they request to join the VATRUS division, data is transmitted from VATSIM centrally to VATRUS for the purpose of ensuring the efficient functioning of our services. This data includes:

- The member's full name
- Their email address
- Their country of residence
- Their age band
- The simulated Air Traffic Control and/or Pilot Rating they have obtained with the VATSIM network
- Positions of responsibility they hold with the network, including level of access

Whilst using our services, additional data is collected from and about you. This allows us to provide the efficient functioning of our services. This data includes:

- IP address and connection info
- Records of webpages visited and services utilised
- Individual training records
- Your requests for support
- Disciplinary history
- Communications with other members
- Any data you submit to our systems through forms or actions taken while using any of our services.

VATRUS собирает ряд персональных данных о своих участниках, как предоставленных участниками напрямую, так и от третьих лиц.

Когда участник пользуется сервисами VATRUS или когда он запрашивает присоединение к дивизиону VATRUS, данные передаются из VATSIM централизованно в VATRUS с целью обеспечения эффективного функционирования наших сервисов. Эти данные включают в себя:

- ФИО участника
- Его адрес электронной почты
- Его страну проживания
- Его возрастную группу
- Рейтинг виртуального диспетчера УВД и/или пилота, полученные им в сети VATSIM
- Должности, которые он занимает в сети, включая его уровень доступа

Во время использования наших сервисов, дополнительные данные собираются от и о вас. Это позволяет нам обеспечить эффективное функционирование наших сервисов. Эти данные включают в себя:

- IP-адрес и информация о соединении
- Записи посещенных веб-страниц и использованных сервисов
- Записи индивидуальных учебных занятий
- Ваши запросы на поддержку
- Дисциплинарная история
- Общение с другими участниками
- Любые данные, которые вы отправляете в наши системы с помощью форм или действий, предпринимаемых при использовании любых наших услуг.

Communication platforms, including our forum, have the functionality to receive any data, in the form of freetext. Any personal data willingly submitted here by individuals (e.g. personal data such a telephone numbers or addresses) will be retained and stored, even if removed from public view. This data is then only available to a limited number of authorised individuals.

VATRUS has an unequivocal commitment to:

- Comply with both the law and good practice
- Respect individuals' rights including:
  - The right of access
  - The right of rectification
  - The right to object
  - The right to suspend protest
  - The right of erasure
- Be open and honest with individuals whose data is held
- Provide guidance for staff who handle personal data, so that they can act confidently and consistently
- Report any cases where the transfer of user data has occurred voluntarily to the appropriate data protection authorities, even if this is not required by law.

Коммуникационные платформы, включая наш форум, имеют функциональность для получения любых данных в виде свободного текста. Любые личные данные, добровольно представленные здесь физическими лицами (например, личные данные, такие как номера телефонов или адреса), будут сохранены и накоплены, даже если они будут удалены из публичного просмотра. Эти данные доступны только ограниченному числу авторизованных лиц.

VATRUS безоговорочно обязуется:

- Соблюдать как закон, так и общепринятую практику
- Уважать права людей, в том числе:
  - Право доступа
  - Право исправления
  - Право на возражение
  - Право приостановить протест
  - Право на удаление
- Быть открытым и честным с людьми, чьи данные сохранены
- Предоставлять рекомендации для сотрудников, которые обрабатывают личные данные, чтобы они могли действовать уверенно и последовательно
- Сообщать о любых случаях, когда передача пользовательских данных произошла добровольно в соответствующие органы по защите данных, даже если это не требуется по закону.

Overall responsibility for ensuring data protection and overall compliance with the relevant standards and legislation rests collectively with the VATRUS Division Staff Group (DSG).

The appointed Data Protection Officer is listed on the VATRUS staff page here: https://vatrus.info/article/6.

Several members of the DSG have specific responsibilities to oversee others accessing personal data collected by VATSIM:

- Division Training Director (VATRUS3) - ATC Training Records;
- Pilots Department Training Director (VATRUS10) - Pilot Training Records;
- Division Information Services Director (VATRUS7) and Information Services Root Administrator (VATRUS8) - Remote access to, and control of stored data.

Other members of the DSG may from time to time be tasked with specific responsibilities pertaining to the control and storage of data.

All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work within VATRUS as detailed in this policy. VATRUS expect the highest standard of probity of all staff at all levels. No access to data can take place unless there is a valid reason for such access.

VATRUS has a zero-tolerance policy towards inappropriate access to data stored within our systems. Any such access will result in the individual concerned being prohibited from having further access until such a time that the risk to personal data has been suitably mitigated.

Вся ответственность за обеспечение защиты данных и полное соблюдение соответствующих стандартов и законодательства лежит на руководстве дивизиона VATRUS (далее - “Руководство Дивизиона”).

Назначенный сотрудник по защите данных указан на странице руководства дивизиона по адресу https://vatrus.info/article/6.

Некоторые члены руководства дивизиона несут определенные обязанности, связанные с доступом к персональным данным, собранным VATSIM:

- Директор учебно-тренировочного центра (VATRUS3) - учебные записи УВД;
- Директор учебно-тренировочного центра по подготовке пилотов (VATRUS10) - отчеты по обучению пилотов;
- Директор информационной службы дивизиона (VATRUS7) и администратор информационной службы (VATRUS8) - удаленный доступ к хранимым данным и управление ими.

Время от времени другим членам руководства дивизиона могут быть поручены конкретные обязанности, связанные с контролем и хранением данных.

Все сотрудники обязаны прочитать, понимать и принимать любые политики и процедуры, относящиеся к персональным данным, которые они могут обрабатывать в ходе своей работы в VATRUS, как подробно описано в настоящей Политике. VATRUS ожидает высочайшего уровня честности всех сотрудников на всех уровнях. Доступ к данным невозможен, если для такого доступа нет действительной причины.

VATRUS придерживается политики абсолютной нетерпимости в отношении несанкционированного доступа к данным, хранящимся в наших системах. Любой такой доступ приведет к тому, что соответствующему лицу будет запрещено иметь дополнительный доступ до тех пор, пока риск для персональных данных не будет соответствующим образом уменьшен.

This section applies to all VATRUS's servers belonging to or donated to the VATRUS division, including, but not limited to Data Servers, Statistic Servers, or Web Servers.

VATRUS operates on a segmented security approach, where only the access required (with approved members holding the status of privileged access) to complete a required job is granted. VATRUS employs access monitoring systems to ensure that access is not being abused and can be traced back to a specific individual.

VATRUS employs standard methods of encryption to safeguard data, such as TLS encryption for accessing data via a web browser. VATRUS also implements additional change-audit scripts and monitors to provide visibility into server activity. IP Address and asymmetric based security settings are used to only allow server access to authorised users or servers. Passwords (excluding your VATSIM password which is never passed to VATRUS) are stored as salted hashes, preventing them from being viewed in plain text.

In order to ensure service continuity, VATRUS retains data backups of relevant systems to ensure a speedy recovery of impacted systems while maintaining data integrity and security. These backups are encrypted, and access is granted only to authorised individuals.

The main specific risks to the security of data are:

- Phishing attacks to gain server level access,
- Access by means of trojan or keylogging programs on members systems, and

Этот раздел относится ко всем серверам VATRUS, принадлежащим или подаренным дивизиону VATRUS, включая, помимо прочего, серверы данных, серверы статистики или веб-серверы.

VATRUS работает на основе сегментированного подхода к обеспечению безопасности, когда предоставляется только необходимый доступ (только авторизованным участникам, имеющим статус привилегированного доступа) для выполнения требуемой работы. VATRUS использует системы контроля доступа, чтобы гарантировать, что отсутствует злоупотребление доступом, и для возможности отслеживания действий до определенного человека.

VATRUS использует стандартные методы шифрования для защиты данных, такие как TLS для доступа к данным через веб-браузер. VATRUS также реализует дополнительные сценарии аудита изменений и мониторинга для обеспечения наблюдения активности сервера. IP-адрес и асимметричные параметры безопасности используются, чтобы разрешить доступ к серверу только авторизованным пользователям или серверам. Пароли (за исключением вашего пароля VATSIM, который никогда не передается в VATRUS) хранятся в виде “хэшей с солью”, что предотвращает их просмотр в виде простого текста.

Чтобы обеспечить непрерывность обслуживания, VATRUS сохраняет резервные копии данных соответствующих систем, чтобы обеспечить быстрое восстановление затронутых систем при сохранении целостности и безопасности данных. Эти резервные копии зашифрованы, и доступ предоставляется только авторизованным лицам.

Основными специфическими рисками для безопасности данных являются:

- Фишинговые атаки для получения доступа на уровне сервера,
- Доступ с помощью троянских программ или программ кейлогинга в системах участников, и

- Access by unauthorised staff members who have been granted access

Mitigation of the first two risks is firstly by screening all individuals before granting access and secondary, encouraging members who have a higher level of access to ensure they adhere to good security practices on their personal systems. The last risk is mitigated by access logging and reverting changes made by those who misuse access.

- Доступ неавторизованных сотрудников, которым ранее был предоставлен доступ

Снижение первых двух рисков - это, во-первых, проверка всех лиц перед предоставлением доступа, а во-вторых, поощрение членов, которые имеют более высокий уровень доступа, чтобы убедиться, что они придерживаются хороших методов безопасности в своих личных системах. Последний риск снижается за счет регистрации доступа и отмены изменений, внесенных теми, кто злоупотребляет доступом.

DATA RECORDING AND STORAGE

The majority of membership data is passed to VATRUS by VATSIM. We assume that these data is accurate. Where it is not, VATRUS offers mechanisms for rectification of membership data, as set out in this policy.

A VATSIM member may request an update of his/her retained information by making a request in writing to members@vatrus.info.

Data is stored in standard file systems and databases. Access to these systems is controlled by secure direct access to the controlling machine or application, or via a secure web interface. Access is further controlled and protected against unauthorized access using standard measures, such as role-based access control.

VATRUS is bound by the retention periods of VATSIM, set out in their Data Protection and Handling Policy. Requests for erasure can be processed by VATRUS but may need escalating to VATSIM in order to fulfil the entirety of the request.

VATRUS does not archive any data to other servers at this point in time for long term storage. Data is either maintained within the production environment and backed up as described above, or deleted entirely.

ЗАПИСЬ И ХРАНЕНИЕ ДАННЫХ

Большая часть данных об участнике передается VATRUS из VATSIM. Мы предполагаем, что эти данные точны. В случаях, где это не так, VATRUS предлагает механизмы исправления данных участника, как изложено в настоящей Политике.

Участник VATSIM может запросить обновление своей сохраненной информации, направив письменный запрос на members@vatrus.info.

Данные хранятся в стандартных файловых системах и базах данных. Доступ к этим системам контролируется безопасным прямым доступом к управляющему компьютеру или приложению, а также через безопасный веб-интерфейс. Доступ дополнительно контролируется и защищается от несанкционированного доступа с использованием стандартных мер, таких как контроль доступа на основе ролей.

VATRUS ограничен периодами хранения VATSIM, указанными в их Политике защиты и обработки данных. Запросы на удаление могут быть обработаны VATRUS, но, возможно, потребуется передача запроса в VATSIM для обеспечения полноты выполнения запроса.

В настоящее время VATRUS не архивирует никакие данные на другие серверы для длительного хранения. Данные либо хранятся в рабочем окружении, либо создаются резервные копии, как описано выше, либо полностью удаляются.

VATRUS is committed to ensuring all members are aware of what data is collected and why we do so. As outlined in the VATRUS Privacy Policy, data is collected for the purpose of ensuring the provision of, and smooth operation of the VATRUS division. Data may be transferred to other organisations affiliated with, or associated with, the division to provide services to enhance and extend the simulated aviation environment. Who we transfer data to is covered within the VATRUS Privacy Policy. Where it is not covered, we will seek your permission to pass on personal data before doing so.

All staff within VATRUS are responsible for the data they access at all times. The various departments most closely associated with members' data are the Web Services Department and Division Staff Group. Where staff are required to use data for statistical and management purposes, anonymous aggregated or pseudonymised data will be used where possible.

VATRUS стремится к тому, чтобы все участники знали, какие данные собираются и почему мы это делаем. Как указано в Политике конфиденциальности VATRUS, данные собираются с целью обеспечения предоставления и бесперебойной работы дивизиона VATRUS. Данные могут передаваться другим организациям, относящимся или связанным с дивизионом, для предоставления услуг по улучшению и расширению моделируемой авиационной среды. На организации, которым передаются данные, распространяется политика конфиденциальности VATRUS. В других случаях, мы будем запрашивать у вас разрешение на передачу персональных данных, прежде чем сделать это.

Все сотрудники VATRUS несут ответственность за все данные, к которым они имеют доступ. Различные отделы, наиболее тесно связанные с данными участников, - это информационная служба дивизиона и руководство дивизиона. Там, где сотрудники должны использовать данные для статистических и управленческих целей, будут по возможности использоваться анонимные агрегированные или псевдонимные данные.

Requests for personal data under the Right of Access are the responsibility of the appointed Data Protection Officer and their team. Such requests are required to be complied with within one month of the request being received. If circumstances prevent this from occurring, an extension of a further two months may be instituted by VATRUS, providing that the member making the request is informed of this fact before the expiration of the original one month deadline.

Right of access requests must be sent via email to web@vatrus.info. If staff at a lower level receive anything that might reasonably be construed to be a request for access they have a responsibility to pass this to the appointed Data Protection Officer, as described above.

Where the person managing the access procedure does not know the individual personally, the individual's identity must be verified before handing over any information.

VATRUS will not charge any fee for processing or providing data for requests under the Right of Access.

The appointed Data Protection Officer is responsible for handling requests under the Right of Access provisions. Requests will be made via web@vatrus.info. Only personal data will be shared with the member. Other individuals' personal data will be redacted.

Запросы на предоставление персональных данных в рамках права доступа являются обязанностью назначенного сотрудника по защите данных и его команды. Такие запросы должны быть выполнены в течение одного месяца с момента получения запроса. Если обстоятельства не позволяют этому произойти, VATRUS может назначить продление еще на два месяца, при условии, что участник, делающий запрос, будет проинформирован об этом факте до истечения первоначального срока в один месяц.

Запросы о праве доступа должны быть отправлены по электронной почте на адрес web@vatrus.info. Если сотрудники более низкого уровня получают что-либо, что может быть разумно истолковано как запрос на доступ, они обязаны передать это назначенному сотруднику по защите данных, как описано выше.

Если лицо, управляющее процедурой доступа, не знает участника лично, его личность должна быть проверена перед передачей какой-либо информации.

VATRUS не будет взимать никакой платы за обработку или предоставление данных для запросов в соответствии с правом доступа.

Назначенный сотрудник по защите данных отвечает за обработку запросов в соответствии с положениями о праве доступа. Запросы необходимо направлять на web@vatrus.info. Только личные данные будут переданы участнику. Персональные данные других лиц будут удалены.

RIGHT OF RECTIFICATION

Accurate data is in the best interests of both the network and the membership. The appointed Data Protection Officer is responsible for the management of such requests.

Right of rectification requests should be made to web@vatrus.info. If staff at a lower level receive anything that might reasonably be construed to be a request for rectification they have a responsibility to direct the member to the above email address.

VATRUS will not charge any fee for requests under the Right of Rectification.

ПРАВО НА ИСПРАВЛЕНИЕ

Точные данные отвечают интересам как сети, так и ее участников. Назначенный сотрудник по защите данных отвечает за управление такими запросами.

Запросы о праве на исправление следует направлять на web@vatrus.info. Если сотрудники более низкого уровня получают что-либо, что может быть разумно истолковано как запрос на исправление, они обязаны направить участника на указанный выше адрес электронной почты.

VATRUS не будет взимать плату за запросы в соответствии с правом на исправление.

RIGHT OF ERASURE

Requests for deletion of personal data under the Right of Erasure are the responsibility of the appointed Data Protection Officer and their team. Such requests are required to be complied with within one calendar month of the request being received. If circumstances prevent this from occurring, an extension of a further two months may be instituted by

VATRUS, providing that the member making the request is informed of this fact before the expiration of the original one-month deadline.

The appointed Data Protection Officer is responsible for handling requests under the Right of Erasure provisions. Requests will be made via web@vatrus.info. If staff at a lower level receive anything that might reasonably be construed to be a request for erasure they have a responsibility to pass this to the appointed Data Protection Officer without delay.

Where the person managing the erasure procedure does not know the individual personally, the individual's identity will be verified before handing over any information.

VATRUS will not charge any fee for deleting data under the Right of Erasure.

ПРАВО НА УДАЛЕНИЕ

Запросы на удаление персональных данных в рамках права на удаление являются обязанностью назначенного сотрудника по защите данных и его команды. Такие запросы должны быть выполнены в течение одного календарного месяца с момента получения запроса. Если обстоятельства не позволяют этому произойти, VATRUS может назначить продление еще на два месяца, при условии, что участник, делающий запрос, будет проинформирован об этом факте до истечения первоначального срока в один месяц.

Назначенный сотрудник по защите данных отвечает за обработку запросов в соответствии с положениями о праве на удаление. Запросы необходимо направлять на web@vatrus.info. Если сотрудники более низкого уровня получают что-либо, что может быть разумно истолковано как запрос на удаление, они обязаны незамедлительно передать это назначенному сотруднику по защите данных.

Если лицо, управляющее процедурой удаления, не знает участника лично, его личность должна быть проверена перед передачей какой-либо информации.

VATRUS не будет взимать никакой платы за удаление данных в соответствии с правом удаления.

VATRUS shall evaluate all requests for erasure. VATRUS reserves the right to retain any data that it believes is in its legitimate interest to do so, or that is required to establish, exercise, or defend any legal claims.

VATRUS оценит все запросы на удаление. VATRUS оставляет за собой право сохранять любые данные, которые, по его мнению, соответствуют его законным интересам или которые необходимы для установления, осуществления или защиты любых юридических требований.

FINAL PROVISIONS

ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

The VATRUS website contains links to other websites. Please be aware that VATRUS is not responsible for the policies of such sites. VATRUS encourages its visitors to be aware when they leave its website and to read the privacy statements of each website that collects personally identifiable information. This Policy applies solely to information collected by VATRUS and its services.

This Policy is an internal document of the personal data operator, is publicly available and is to be posted on the official website of VATRUS - https://www.vatrus.info/.

This Policy is subject to change, addition in case of new legislation and special regulatory documents.

This Policy was prepared in Russian and in English. If any contradiction exists between the Russian version of this Policy and the English version, the Russian version will prevail.

Сайт VATRUS содержит ссылки на другие сайты. Помните, что VATRUS не несет ответственности за политики таких сайтов. VATRUS призывает своих посетителей быть в курсе, когда они покидают веб-сайт VATRUS, и читать заявления о конфиденциальности и политики защиты и обработки данных каждого веб-сайта, который собирает личную информацию. Настоящая Политика относится исключительно к информации, собранной VATRUS и его сервисами.

Настоящая Политика является внутренним документом оператора персональных данных, является общедоступной и подлежит размещению на официальном сайте VATRUS - https://www.vatrus.info/.

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов.

Настоящая Политика подготовлена на русском и английском языке. В случае обнаружения каких-либо несоответствий между версией настоящей Политики на русском языке и версией настоящей Политики на английском языке определяющее значение будет иметь версия на русском языке.