OUR SECURITY POLICY & GDPR

We take security of your Web based Expense Management system very seriously:

Web based Expenses, Hosted Expenses, On-line Expense, Cloud Computing, Software as a Service and Software on Demand are all words which describe the same concept: Secure access to your Expense On Demand (EOD) system at any computer, anywhere, anytime over the internet via your web browser.

Servers are hosted in the UK by one of the world's leading infrastructure organisations. There is no client software required on the desktop or on the user's network. This means that new users can be activated easily and very quickly.

Keeping your data safe:

1. You exclusively own your own data in your EOD system. Should you no longer wish to use EOD, you can easily export all your data to text files or spread sheets and import it into another system.
2. Your data is safe with EOD. In fact, far safer than most in-house applications because, without a valid password, data cannot be selected or downloaded.
3. The minute you login into your EOD subscription, the highest level encryption kicks-in, i.e., SSL 256K (AES) - this means that your data travels over the internet fully encrypted.

Our security:

1. We take security very seriously. As a UK registered company, we are governed by the UK Data Protection Act's requirements – arguably one of the most stringent regimes in the world. This certification has to be renewed each year.
2. Indeed, in line with best practice, we regularly conduct an audit of our facilities and the EOD service. To this end, we carry out penetration tests and a vulnerability assessment once every quarter, not only of the application but also of the networks and the infrastructure.
3. Access to the application is via SSL 256K AES encryption.
4. Access to your subscription is via a secure password.
5. The database access is funnelled through one class that handles all of the interaction with the SQL Server Managed provider. The data within SQL Server is stored in separate databases for each client. This is referred to as the isolated model in Microsoft's Multi-Tenant Data Architecture. The overview can be found here http://msdn.microsoft.com/en-us/library/aa479086.aspx.
6. Within each client database, data is accessed via stored procedures held in the database to ensure complete isolation of data access between clients. When data is added via the EOD web application, the data is encrypted in the data layer using SQL functions and a client specific private key before it is written to the database ensuring all sensitive data is encrypted at field level during rest. Only the requested data is decrypted when it is accessed via the EOD web application. EOD incorporates full database level encryption by utilising SQL Server 20xx transparent data encryption technology. This allows all database files (data and log) to be encrypted while stored on disk. TDE is the optimal choice for bulk encryption to meet regulatory compliance or corporate data security standards. Using both of these technologies provides EOD with dual layer security, external database file encryption with private key and internal database field level data encryption, also with a (separate) private key.

100% Availability:

1. Your data is backed up every day and backups are retained for 28 days on a rolling basis. Back-up files are retained on separate devices at the same location and remote locations, with full DR capability in place.
2. Our EOD servers are held in highly secure, purpose built facilities, and are managed around the clock. Our servers are always kept updated with the latest security patches.
3. Redundant Cisco routers and stateful inspection firewalls are configured in fail over mode.
4. The servers have two redundant 1 Gbyte fibre Internet connections and redundant power supplies and fire protection.
5. A 12.5 MVA diesel generator stands by in case of a power cut with fuel on site to provide at least 24 hours running at full design and SLA for refuelling within 6 hours of call-out. Generators are configured to automatically fail-over.
6. Secure and separate VLAN for database & application/web servers.
7. Server load balancing and clustering has been implemented to ensure high availability
8. Implementation of SAN to allow multiple servers to access the data. Each server has multiple data paths.
9. Redundancy for precision HVAC, power and fire detection/suppression systems, etc.
10. Data is stored using raid disk technology, with a daily back-up to a secondary location. We use https secure socket layer to ensure encryption of all communications.
11. Multi-level physical security. All areas of the centre are monitored and recorded using CCTV, and all access points are controlled.

12. Software version control, device configuration control, user access privileges and security are standard features of our security processes.
13. Secure, scalable, and highly available SLA based operations services on a 24x7 basis is supported by our infrastructure operations management team.
14. Infrastructure is actively monitored to provide a system-level perspective of support systems, network devices, application servers, web servers, databases, and virtually any component of infrastructure through the following:
    a. Multiple layers of hardened physical security
    b. “Man trap” entry
    c. 24x7x365 on-site security presence
    d. Closed-circuit television surveillance in reception and hallways
    e. Multiple layers of electronically controlled card access
    f. Card swipe system
    g. Authorized staff only based on access list who are adequately trained in the Data Protection Legislation and the handling of Personal Data
    h. Facility-issued photo IDs
    i. Real time 3rd party website monitoring through http://www.gomeznetworks.com is in place.
    j. Robust Escalation and Change management process
    k. Periodic auditing of the infrastructure and equipment and maintenance of Site Run Book in standard format.
15. The infrastructure is ISO 270001 certified, also has the SAS 70 Type II Certification, which is now called SSAE 16.
16. Redundant server groups are configured to automatically failover to ensure zero downtime.

GDPR

The GDPR is coming, and Expense on Demand is here to help.

On May 25, 2018, a new landmark privacy law called the General Data Protection Regulation (GDPR) takes effect in the European Union (EU). The GDPR expands the privacy rights granted to EU individuals, and it places many new obligations on organizations that market to, track or handle EU personal data, no matter where an organization is located. EOD is here to help our customers in their efforts to comply with the GDPR through our robust privacy and security protections.

What is the GDPR?

The GDPR is a new comprehensive data protection law (in effect May 25, 2018) in the EU that strengthens the protection of personal data in light of rapid technological developments, increased globalization, and more complex international flows of personal data. It updates and replaces the patchwork of national data protection laws currently in place with a single set of rules, directly enforceable in each EU member state.

What does the GDPR regulate?

The GDPR regulates the "processing" of data for EU individuals, which includes collection, storage, transfer, or use. Any organization that processes personal data of EU individuals is within the scope of the law, regardless of whether the organization has a physical presence in the EU. Importantly, under the GDPR, the concept of "personal data" is very broad and covers any information relating to an identified or identifiable individual (also called a "data subject").

How does GDPR change privacy law?

The key changes are the following:

1. Expanded data privacy rights for EU individuals, data breach notification and added security requirements for organizations, as well as customer profiling and monitoring requirements.
2. GDPR also includes binding Corporate Rules for organizations to legalize transfers of personal data outside the EU, and a 4% global revenue fine for organizations that fail to adhere to the GDPR compliance obligations.
3. Overall the GDPR provides a central point of enforcement by requiring companies to work with a lead supervisory authority for cross-border data protection issues.

Does the GDPR require EU personal data to stay in the EU?

While GDPR does not require EU personal data to stay in the EU, nor does it place any new restrictions on transfers of personal data outside the EU subject to certain provisions. We at EOD still ensure that EU users data does indeed stay within the EU. Please also read the MSA.

What EOD is Doing:

EOD welcomes the GDPR as an important step forward in streamlining data protection requirements across the EU and as an opportunity for EOD to deepen our commitment to data protection. Similar to existing legal requirements, compliance with the GDPR requires a partnership between EOD and our customers in their use of our services. EOD will comply with the GDPR in the delivery of our service to our customers. We are also dedicated to helping our customers comply with the GDPR.

EOD 's Commitment to Data Protection.

At EOD, trust is our #1 value and nothing is more important than the success of our customers and the protection of our customers' data. EOD 's robust privacy and security program meets the highest standards in the industry. We have consistently reinforced our commitment to protecting our customers' through our actions over the last few years:

What Customers Should Do

1. Get Buy-in and Build a Team
    a. Raise awareness of the importance of GDPR compliance with organization leaders
    b. Obtain executive support for necessary staff resources and financial investments
    c. Choose someone to lead the effort
    d. Build a steering committee of key functional leaders
    e. Identify privacy champions throughout the organization

2. Assess the Organization
    a. Review existing privacy and security efforts to identify strengths and weaknesses
    b. Identify all the systems where the organization stores personal data and create a data inventory
    c. Create a register of data processing activities and carry out a privacy impact assessment for each high-risk activity
    d. Document Compliance

3. Establish Controls and Processes
    a. Ensure privacy notices are present wherever personal data is collected
    b. Implement controls to limit the organization's use of data to the purposes for which it collected the data
    c. Establish mechanisms to manage data subject consent preferences
    d. Implement appropriate administrative, physical, and technological security measures and processes to detect and respond to security breaches
    e. Establish procedures to respond to data subject requests for access, rectification, objection, restriction, portability, and deletion (right to be forgotten)
    f. Enter into contracts with affiliates and vendors that collect or receive personal data
    g. Establish a privacy impact assessments process
    h. Administer employee and vendor privacy and security awareness training

4. Document Compliance
    a. Compile copies of privacy notices and consent forms, the data inventory and register of data processing activities, written policies and procedures, training materials, intra-company data transfer agreements, and vendor contracts
    b. If required, appoint a data protection officer and identify the appropriate EU supervisory authority
    c. Conduct periodic risk assessments

GDPR: Fiction versus Fact

As you gear up your organization to comply with the forthcoming EU General Data Protection Regulation (GDPR), you may come across contradictory information about what the GDPR does -- and does not -- require.

One of the main challenges for organizations who are facing GDPR compliance is getting the resources to sort through the facts, and the fictions, of this new law. With that in mind, EOD has put together this guide to help clarify some common confusions around the GDPR and get you and your organization on the path towards compliance.

1. Fiction: "Processing European personal data requires the consent of the data subject."
   Fact: Consent is only one of the legal bases one can use for the processing of personal data (Article 6(1)(a)). For instance, personal data can also be processed:
   a. when necessary for the performance of a contract to which the data subject (the individual whose data is processed) is a party;
   b. when there is a legal obligation to do so (such as the submission of employee data to a tax authority); and
   c. sometimes even on the basis of legitimate interests, such as commercial and marketing goals. The legitimate interest must, however, outweigh any detriment to the privacy of the data subject.

2. Fiction: "European personal data must be stored within Europe."
   Fact: The GDPR does not contain any obligation to store information in Europe. However, transfers of European personal data outside the European Economic Area (EEA) generally require that a valid transfer mechanism be in place to protect the data once it leaves the EEA (Chapter V, Articles 44-50).

3. Fiction: "The GDPR requires EU personal data to be encrypted at rest."
   Fact: The GDPR does not mandate specific security measures. Instead, the GDPR requires organizations to take technical and organizational security measures which are appropriate to the risks presented (Article 32(1)). Encryption at rest and pseudonymization may be appropriate depending on the circumstances, but they are not mandated by the GDPR in every instance. Despite not being mandated, EOD encrypts data at rest, which also includes dates.

4. Fiction: "EU data subjects have an absolute right to have their personal data deleted upon request."
   Fact: The right to have one's data deleted is often referred to as "the right to be forgotten". However, the right to be forgotten is not an absolute right. It has a limited scope and is subject to certain limitations (Article 17). In most cases, when considering a request for deletion several relevant factors have to be taken into account; this right will not apply, for example, if the processing is necessary for compliance with a legal obligation. However, data subjects do have an absolute right to prevent their personal data from being processed for direct marketing purposes.

5. Fiction: "A data protection officer is mandatory for all companies subject to the GDPR."
   Fact: A data protection officer is only required by the GDPR when one of the following applies:
   a. the organization is a government institution;
   b. the organization processes certain sensitive types of data (such as data on health or religion) on a large scale as part of their core activities; or
   c. the organization systematically monitors people (for example, via cameras, or software which tracks internet behavior) as part of their core activities (Article 37(1)).

6. Fiction: "The GDPR requires a data protection impact assessment for all processing activities involving EU personal data."
   Fact: Under the GDPR, a data protection impact assessment (DPIA) is only necessary when it concerns high-risk processing of EU personal data, such as the following:
   a. large-scale processing of certain sensitive types of EU personal data, such as data concerning a person's health;
   b. systematic and extensive automated decision-making which produces legal or similarly significant effects on individuals, such as the use of fraud detection software; and
   c. systematic and large-scale monitoring of public space (for example, with cameras) (Article 35(3)).

7. Fiction: "Profiling and automated decision making is prohibited under the GDPR."

Fact: Profiling of EU individuals and automated decision-making involving EU personal data are not prohibited, but these processing activities may be subject to certain conditions. In particular, when decisions which legally or similarly significantly affect an individual are made automatically, the data subject:

a. must be given meaningful information about the underlying logic, and about the significance and potential consequences for them; and
b. must in some cases have the ability to require that a human being is involved in the process (Article 22(3)). A data protection impact assessment (see Myth 6 above) may also be required.

8. **Fiction**: "If an organization is established outside the EU, the GDPR does not apply to its processing of EU personal data."
Fact: Regardless of where an organization is established, the GDPR applies to EU personal data which is processed in the context of:

a. offering goods and services (whether paid or not) to people in the EU; or
b. monitoring the behavior of people in the EU, for example by placing cookies on the devices of EU individuals (Article 3(2)).

This document is a broad overview of some of the key aspects of the forthcoming EU General Data Protection Regulation (GDPR) and does not provide legal advice. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

1. Expanded definition of "**personal data**": The GDPR expands and clarifies the concept of personal data. While the basic concept of personal data largely remains the same, the GDPR makes it clear that location data and online identifiers, such as IP addresses, are considered personal data. The GDPR also expands the concept of sensitive personal data to include genetic data and biometric data.
2. Expanded and new rights for EU individuals: The GDPR provides expanded rights for EU data subjects such as:
    a. Deletion: This right is sometimes referred to as the "right to be forgotten". The data subject has the right to require that the Controller erase personal data about him/her in certain conditions, including if the personal data is no longer necessary for the original purpose of the processing or if the data subject withdraws consent for the processing. This right has been extended to the online world as a means to require internet service providers to delete out-of-date publicly available information, in particular that information which appears in search results.
    b. Restriction: Under the GDPR, a data subject has the right to obtain from a Controller a restriction on the processing of personal data in a number of circumstances, including if the accuracy of the personal data is contested by the data subject for a certain period of time. A restriction on processing means that the organization holding the data is entitled to continue to store it, but cannot process it any further.
    c. Portability of personal data: Data subjects also now have the right, in certain circumstances, to receive the personal data that they have provided to a Controller in a structured, commonly used and machine-readable format.

3. Security measures: The GDPR requires Controllers and Processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented. At EOD, we have robust security measures in place that meet the highest standards in the industry, and these our outlined in our Security Policy.

4. Breach notification: The GDPR requires organizations to report certain personal data breaches to the relevant data protection authority, and in some circumstances, to the affected data subjects. Controllers must notify the relevant data protection authority "without undue delay" (and where feasible, within 72 hours of having become aware of it), unless the breach is not likely to present any risk to the rights and freedoms of the data subjects concerned. If circumstances require it, Controllers may also be required to communicate the data breach to data subjects. Processors, for their part, are required to notify Controllers "without undue delay" after becoming aware of a personal data breach. EOD has covered these aspects in its MSA.

5. Transparency: The GDPR requires that Controllers provide data subjects with information about their processing operations at the time when the personal data are collected. This information includes the identity and contact details of the Controller, the contact details of the data protection officer (if relevant), the purposes and the legal bases for the processing of the personal data, the recipients of the data and a number of other fields to ensure that the personal data is being processed in a fair and transparent manner. In addition, Controllers are required to provide information to data subjects even in circumstances where the personal data has not been obtained directly from the data subject.

6. Profiling: The GDPR introduces the concept of "profiling" or any form of automated processing that uses personal data to evaluate personal aspects and in particular to analyse or predict aspects relating to an individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Data subjects must be informed of the existence of profiling and any consequences of the profiling. EOD does not profile any of the above.