

Roush
Employee Personal Data Privacy and Security Statement

Roush is committed to providing privacy protection of employee data maintained by the company. It is Roush's intention to comply with all local data protection regulations worldwide including the European Commission's Directive on Data Privacy, which took effect in October of 1998. The company will certify annually with the U.S. Department of Commerce that Roush Industries, Inc. is in compliance with the safe harbor framework approved by the European Union. Compliance with the safe harbor framework demonstrates the adequate privacy protection required by the European Commission's Directive.

Notice: Roush maintains a global Human Resource Information System (HRIS) to manage and administer the company's human resources. The database for the HRIS is located at Roush's North American data center in Livonia, Michigan. Personal information is stored in Roush's computer database (PeopleSoft), as well as in hard copy format, i.e. employee personnel jacket. The primary purpose for collecting this data is to automate Roush's payroll and job-costing process.

The personal information that Roush collects includes:

- Name
- National Insurance #
- Home Address
- Salary
- Highest Education Level
- Marital Status
- Gender
- Telephone Number
- Benefits Plan
- Date of Birth
- Emergency Contact Information
- Mobile Phone #

Choice: Roush collects no personal information about employees unless provided to Roush by completion of a written consent form, employment forms and questionnaires, participation in a survey or completion an on-line form or hard copy form. Employees may choose to submit personal, private information by fax, via e-mail or regular mail. If an employee refuses to provide consent, Roush will not store their personal information in the database.

Onward Transfer: Roush will not disclose or share employees' personal information with any outside entity or third party administrator.

Security: The importance of security for all personally identifiable information associated with Roush employees is of utmost concern. Roush has taken several steps to safeguard the integrity of personal information and prevent unauthorized access to information maintained in our database. These measures are designed and intended to prevent corruption of data, block unknown and unauthorized access to our HRIS system and information, and to provide reasonable protection of private, personal information in Roush's possession. Access to the HRIS database is controlled by a log-in sequence and requires users to identify themselves and provide a password before access is granted. Users are limited to data required to perform their job function. Security features of the HRIS software and developed processes are used to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration and destruction.

PeopleSoft Security: Access to our PeopleSoft database is strictly controlled by the Security Administrator and it is based on the employee's role in the company.

Data Integrity: Personal information should be accurate and complete. Personal information is initially collected at the time an employee is hired. Further, the HR Dept. mails a "Personal Data

Verification" form letter once a year to all active employees. If any information on the Personal Data Verification form is incorrect, employees are asked to update it and return to the HR Department. Upon receipt of this form, Roush will make the appropriate changes in the database.

Access: Only those employees in the HR Dept. who need access to employee personal information in order to do their job have access to view that information that is stored in our database. Further, all employee personnel jackets are kept on file in the HR Department, in locked file cabinets. No Roush manager may view an employee's file without requesting it from a member of the HR Dept. All personnel files remain on site in the HR Dept., personnel jackets are not permitted to be removed by a Roush manager. An employee may view their own personnel record upon request by contacting the Roush Europe HR Department.

Enforcement: Any employee who violates Roush's privacy and/or security policies is subject to disciplinary action, up to and including termination and civil and/or criminal prosecution. Annual reviews of this policy and principles will take place as part of the certification process with the U.S. Department of Commerce. Roush will include internal compliance reviews as part of the company's internal self-audit process. Employees should forward any complaints or disputes regarding personal data protection to their local HR representative. Complaints or disputes that cannot be remedied by the local HR representative should be forwarded to the Human Resource Manager located at:

Roush Industries, Inc.
11873 Market Street
Livonia, Michigan USA 48150

Roush agrees to cooperate with U.K. data protection authorities to resolve disputes with employees that cannot be remedied directly with the employee.