GDPR Dataflow Matrix – Microsoft User Stories
July 2017

	User Type	Data Elements	Purpose Specification	Other Info
1	As an SSL Cert Admin	I use registrant name, address, email address and creation date	to validate domain name ownership for SSL cert requests	We only issue certificates for domains owned by Microsoft Corporation
2	As a TM rights holder	I use registrant name, address, email address and creation date	for enforcement purposes against registrants who are infringing our Intellectual Property rights.	Registrant contact information can be used for purposes of sending a cease and desist letter to a website owner that has infringing content on their website, but the domain itself is not infringing; In instances where the domain itself is infringing and based on location of the registrant, we may decide to first send a C&D letter prior to filing a UDRP complaint to recover the domain. Registrant's email address is also used for purposes of running a ReverseWhois report to see if the same registrant owns any other domains that infringe our IP rights.
3	As a Corporate Domains Admin	I use Name Servers to check which DNS system is authoritative for a given domain name	to verify whether a Microsoft domain name is hosted by a Microsoft-owned name server platform	We also frequently use DIG or CentralOps for this

4	As a Corporate Domains Admin	I use transfer EPP key, domain status, domain creation date and expiry date, admin contact email address, nameservers/DNS records	to facilitate domain name transfers to and from third party registrants	
5	As a Corporate Domains Admin	I use registrant name, address, email address and creation date	to address internal inquiries and assist in domain ownership investigations	General inquiries come to CorpDomains from numerous teams across the Company
6	As a Corporate Domains Admin	I use registrant name, address, email address and creation date	To run a Reverse Whois report to gather information about a domain name's ownership history to help inform acquisition projects	
7	As a potential registrant	I use domain name, registrar, deletion date	To help determine if domain name is available for registration, or when it is scheduled to expire	
8	As a Digital Crimes Investigator	I leverage this type of information for each type of individual cited in WHOIS: • Registrant • Admin contact • Tech contact We use the following data fields: • Name • All address fields (street address, city, state/region, country, postal code, etc.) • Phone number • Email address • ID fields	To investigate a malware incident and/or assisting in the investigation related to a malware operation, I use WHOIS to identify: • if a domain is registered • when the domain was registered and when it expires • the Registry with whom the domain was registered • if the domain is used for service such as dynamic DNS • Name Servers for a domain • the Registrant contact information such as name, address, phone #, and email. This information's is used during the discovery process when DCU has a court	Microsoft devotes significant resources to combating online fraud and abuse, and threats to online safety. In addition to Microsoft's activities to combat online piracy, counterfeiting, and cybersquatting, Microsoft works to disrupt some of the most difficult cybercrime threats facing society today – including technology-facilitated child sexual exploitation and malicious software crimes, particularly botnet-driven Internet attacks. Microsoft personnel routinely use and rely on WHOIS data in these important efforts. For example, one of the most accurate purpose

			approval to size the domain and notify the domain owner • technical contact information such as name, address, phone #, and email. Often, this information is used to report abuse such as Phishing or potential breach.	that describes Microsoft personnel's use of WHOIS data is "abuse mitigation," and in the case of the Digital Crime Unit's malware operations, the identification of malware infrastructure for the purpose of identifying and remediating millions of infected victims. We have observed a tendency of the criminals to re-use some of the same information when registering their domains. For example, we have seen registrants changing the name of the individual, but using the same (often bogus) address and/or email address and/or phone number. We have also seen distinctive patterns, such as using similar addresses (i.e. "2050 main street, suite 1A", then "suite 1C", then "suite 4A") with different names. By reviewing WHOIS information, we are able to determine multiple domains registered by the same entity and sometimes are able to predict where harm will next be occurring in advance of the malicious activity.