4.4. However, such Processing must be in a manner that complies with ~~GDPR~~ applicable data protection laws, including on the basis of a specific identified purpose for such Processing. Accordingly, Personal Data included in Registration Data may be Processed on the basis ~~of a~~ for the purpose of domain name registrations in compliance with applicable data protection laws, ~~legitimate interests not overridden by the fundamental rights and freedoms of individuals whose Personal Data is included in Registration Data~~ and only for the following legitimate purposes:

4.4.1. Reflecting the rights of a Registered Name Holder in a Registered Name and ensuring that the Registered Name Holder may exercise its rights in respect of the Registered Name;

~~4.4.2. Providing access to accurate, reliable, and uniform Registration Data based on legitimate interests not outweighed by the fundamental rights of relevant data subjects, consistent with GDPR;~~ [1]

4.4.3. Enabling a reliable mechanism for ~~identifying and~~ contacting the Registered Name Holder for a variety of legitimate purposes more fully set out below;

~~4.4.4. Enabling a mechanism for the communication or notification of payment and invoicing information and reminders to the Registered Name Holder by its chosen Registrar;~~ [2]

4.4.5. Enabling a mechanism for the communication or notification to the Registered Name Holder of technical issues ~~and/or errors~~ with a Registered Name~~, or any content or resources associated with such a Registered Name~~;

~~4.4.6 Enabling a mechanism for the Registry Operator or the chosen Registrar to communicate with or notify the Registered Name Holder of commercial or technical changes in the domain in which the Registered Name has been registered;~~

~~4.4.7 Enabling the publication of technical and administrative points of contact administering the domain names at the request of the Registered Name Holder;~~

4.4.8. Supporting a framework to address issues involving domain name registrations, including but not limited to: ~~consumer protection,~~ law enforcement investigation ~~of cybercrime~~, ~~and~~ DNS abuse, and tailored mechanisms designed to protect intellectual property interests (as provide for by Section 4.4) ~~and intellectual property protection~~;[3]

~~4.4.9. Providing a framework to address appropriate law enforcement needs;~~ [4]

[1] Vaguely worded and omits the concepts of necessity.  Removed here because it belongs more appropriately under the umbrella of an access model.

[2] Communication between a registrar and its customer has nothingto do with WHOIS. Additionally, there is mechanism already in place, https://www.icann.org/resources/pages/errp-2013-02-28-en

[3] Other issues should be discussed during the “Access” phase, as they go beyond the original purpose (domain name registrations) for collecting data. It should be noted, there is already a security framework called SPEC 11 Security framework.

[4] this should be discussed within the “Access” discussion.

~~4.4.10. Facilitating the provision of zone files of gTLDs to Internet users;~~ [5]

~~4.4.11. Providing mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure, or other unavailability of a Registrar or Registry Operator;~~ [6]

4.4.12. Coordinating dispute resolution services for ~~certain disputes concerning domain names~~ URS and UDRP, and;

4.4.13. Handling contractual compliance monitoring requests (which include provisions for contracted parties to invoke non-binding arbitration and other procedures to address conflicts with law), audits, and complaints submitted by Registry Operators, Registrars, Registered Name Holders, and other Internet users.

Notes:

- We recommend that we avoid overly-specific language in Section 4.4, to ensure that Contracted Parties can comply with the Accountability Principle in GDPR, and equivalent provisions in other laws.
- We recommend removing specific references to GDPR from contract language, to ensure compatibility with other, equivalent data protection laws.
- RrSG members have divergent positions on Sec. 4.4.8
- The RrSG team notes that, because ICANN cannot fully indemnify Contracted Parties against penalties under GDPR or other data protection regulations, any ICANN Compliance matter must include provisions for Contracted Parties to invoke non-binding arbitration under the RA or RAA, or other procedure, to address conflicts with applicable law.
  - In the event that arbitration fails to resolve the conflict, the law takes precedence.
  - We include this comment as part of our edits to Section 4.4, but will also raise this point as part of any revision/update of the WHOIS Conflicts Process, as has been noted in previous calls.

[5] The provision of zone files is nothing to do with WHOIS

[6] Addressed by data escrow requirements already in place